Svenskt federationsforum

Internetdagarna 25 nov 2014

Syfte med dagen

- Informera
- Inspirera
- Samverka

SVENSKT FEDERATIONSFORUM

#fedforum14 #ind14

Flera federationer?

Talare idag

Program

10:30 Federationer, trender och utmaningar

Inledningstal Leif Johansson, SUNET

Status för

- Sambi
- Skolfederation
- Svensk e-legitimation
- Eduroam, SWAMID och GÉANT Association

eIDAS, EU:s nya förordning för elektronisk identifiering

12:30 Lunch

13:30 För Internetdagarna gemensam session: Eben Upton

14:00 Erfarenhetsutbyte – Blixttal

- Ladok3, ett nationellt studieadministrativt system utan användarkonton
- Federationsanpassning av Ineras Säkerhetstjänster
- eHälsomyndighetens och Ineras POC för web services
- En Testspecifikation för Sambis test- och demonstrationsbädd
- Appar och federationer
- Säker inloggning och federerade identiteter i appar
- Anslutning av appar till federationer

15:15 Fika

15:45 Blixttal fortsättning

- Varför eduID?
- Ta tillbaka kontrollen över federerade identiteter och data med SCIM
  Erfarenheter från arbetet med att uppnå definierad SWAMID AL1-nivå
- Sambis nya tillitsramverk
- Implementation av eskalerad tillitsnivå från en pilot med Göteborgs stad
- SLL, KSL och Sambi ordnar enklare inloggning

Summering av dagen

- Samverkan

17:00 Mingel, middag och underhållning

Inledningstal

Federationer i ett globalt perspektiv, trender och utmaningar

Leif Johansson, SUNET

Federationer i ett globalt perspektiv, trender och utmaningar

SUNET

The F-word

fed·er·a·tion *noun* \ˌfe-də-ˈrā-shən\

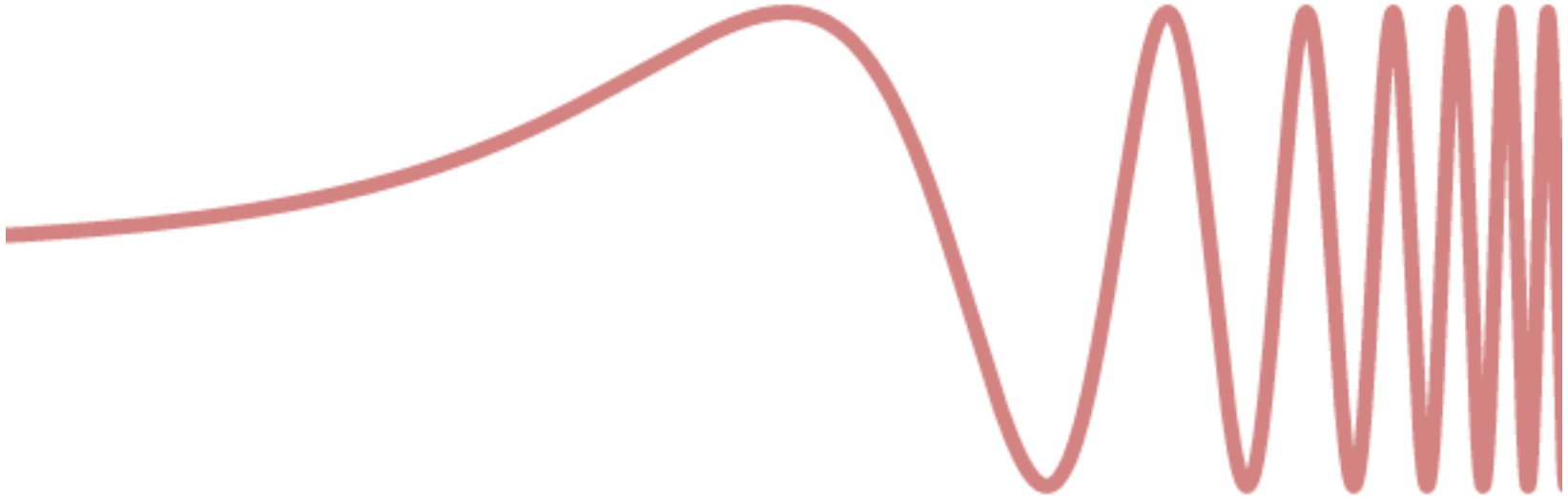
: a country formed by separate states that have given certain powers to a central government while keeping control over local matters

: an organization that is made by loosely joining together smaller organizations

: the act of joining together separate organizations or states

SUNET

The 2014 Federation Hype Cycle



SUNET

The Who

SUNET

SWAMID Instiftas 4 Maj 2007

SUNET


ORCID


CONNECT.GOV


SURFconext


SWAMID


IGTF
AP|EU|TAG


Sambi


umbrella


haka

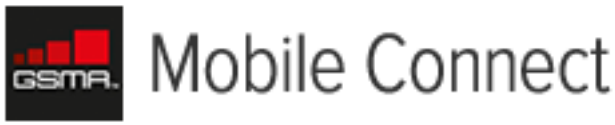

eduGAIN


The UK
Access
Management
Federation
FOR EDUCATION AND RESEARCH


KALMAR 2


InCommon


Skolfederation.se

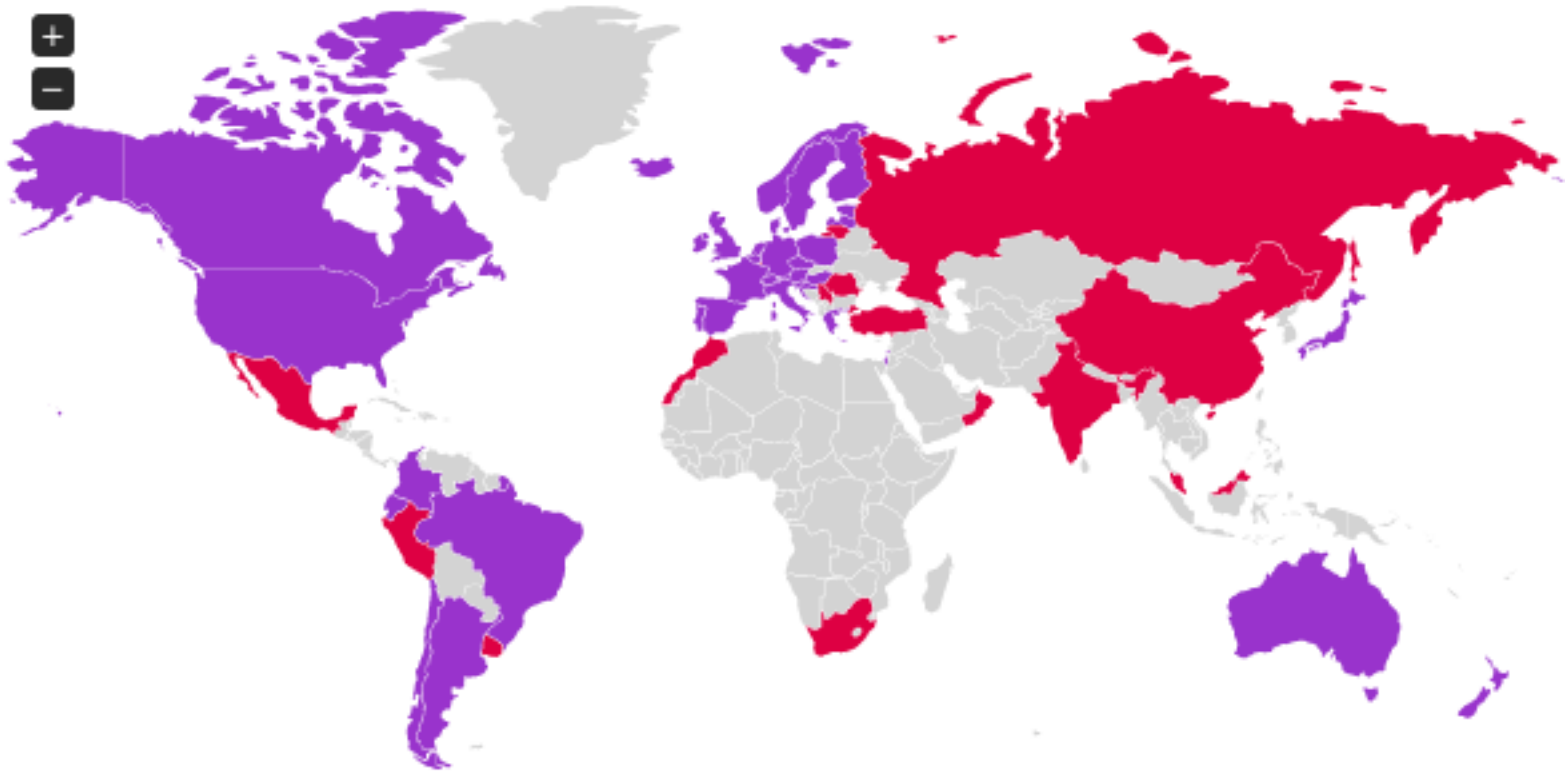

GSMA
Mobile Connect


SAFE-BioPharma


Global Federated Identity and Privilege Management
Sponsored by the U.S. Department of Justice and the U.S. Department of Homeland Security


InAcademia
Simple Affiliation validation for Academia


SUNET



SUNET

“Tjänet”

SUNET

- ID-länkare
- Köpklubb
- (På)Reglering
- Avreglering

SUNET

Länkare	umbrellaid.org, orcid.org, klout.com
Köpklubbar	swamid, skolfederation (?), id.me
Reglering	eLeg, connect.gov
Avreglering	sambi, OpenID Heart WG, gsmamc

SUNET

TODO

SUNET

Attribut & Personinfo

SUNET

Commission proposes a comprehensive reform of the data protection rules

Date: 25/01/2012

Brussels, 25 January 2012 – The European Commission has today proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.

SUNET

OpenID Connect
[paw rihk-titt]

SUNET

Mobile Connect – Overview

September 24, 2014 | Resources, Videos and Webinars | Overview

Introducing Mobile Connect – the convenient and secure login solution with privacy protection:

Förtroenderamverk 2.0

(son-of-NIST 800-63)

SUNET


LoA1: What you have
LoA2: What you can just afford
LoA3: What the MAN tells you
LoA4: Nuclear strike

SUNET

vot@ietf.org

https://www.ietf.org/mailman/listinfo/vot

SUNET

Sambi

Stefan Larsson, eHälsomyndigheten

Sambi

Samverkan
för säkrare
e-hälsa

Statusrapport
Internetdagarna 2014-11-25

Sambi
Samverkan
för säkrare
e-hälsa

Agenda

Statusrapport

1. Pilotperiod
2. Tillitsgranskning
3. Tillitsramverk
4. Föreskrifter för federationsoperatören
5. Förvaltning av behörighetsstyrande attribut

Sambi
Samverkan
för säkrare
e-hälsa

Statusrapport

Pilotperiod

- *SLL*
- *Stockholms Stad*
- *eHälsomyndigheten*
- *SITHS*

- *En handfull idp:er har testats i Sambis testbädd*

Betsällnings-
portalen
(SLL)

Sambi
Samverkan
för säkrare
e-hälsa

Statusrapport

- Tillitsgranskning, 8 case i slutskede av granskning
  - *Danderyds kommun*
  - *eHälsomyndigheten*
  - *SLL Beställningsportalen*
  - *SLL WebCare*
  - *SLL SITHS+Intygsutfärdare*
  - *Stockholms stad*
  - *SITHS (via e-legitimationsnämnden)*
  - *Inera nationell IDP (arbetet påbörjas inom kort)*

Sambi
Samverkan
för säkrare
e-hälsa

Statusrapport

- Utkast till nytt tillitsramerk inom Sambi
  - *Remissats i en mindre grupp (ca 20-talet pers)*
  - *Antas troligen i Sambis styrgrupp 2014-12-02*
  - *Harmoniera med e-leg nämnden …*

Sambi
Samverkan
för säkrare
e-hälsa

Statusrapport

- Föreskrifter för federationsoperatören

Operatörens åtaganden …

- *Medlemshantering*
- *Metadata*
- *Teknisk drift*
- *Attributförvaltning*
- *Tillit och granskning*
- *Ändringshantering*
- *Etc*

Sambi
Samverkan
för säkrare
e-hälsa

Statusrapport

- Förvaltning av behörighetstyrande attribut
  - *Inera har erbjudit sig att ansvara*
  - *Piloterna har hört av sig för dialog*

Statusrapport

Avslutningsvis

Viss vägs vandring för att nå upp till kraven …

Men syftet är ju tillit på riktigt!

Skarpa tjänster under Q1 2015 … ☺

Tack!

Skolfederation

Robert Sundin, .SE

Skolfederation

Svenskt federationsforum

Internetdagarna 2014-11-25

Skolfederation.se

Likheter och olikheter med andra federationer

Skolfederation.se

Skolfederations vision

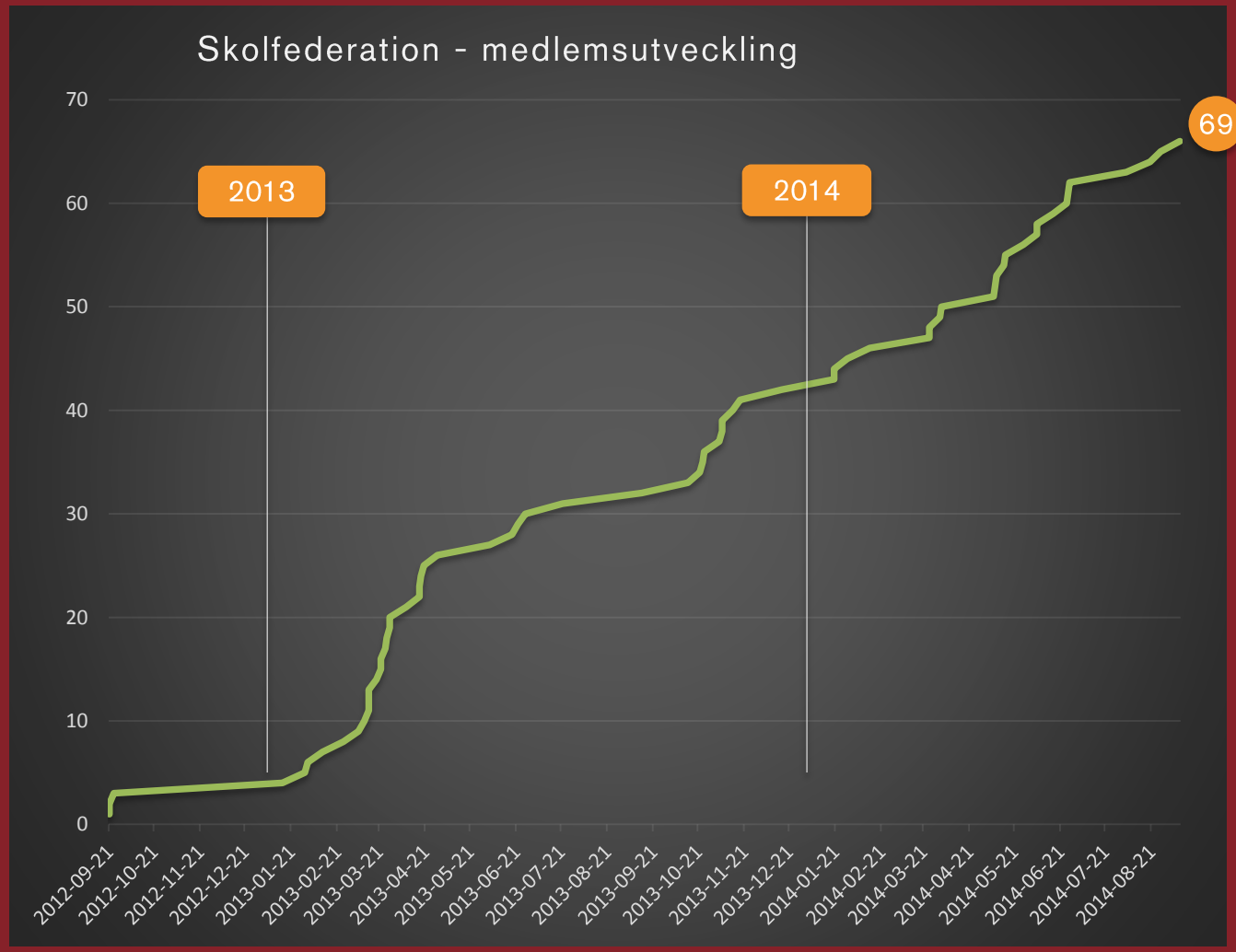
- **En enda inloggning** för enkel och säker tillgång till skolans och leverantörers tjänster.
- Anonymisering för skydda den **personliga integriteten**.
- Ge Skolhuvudmannen en **valfrihet att välja sina egna tjänsteleverantörer och sin egen inloggningslösning**.
- **Underlätta för tjänsteleverantörer** att ansluta nya skolhuvudmän.

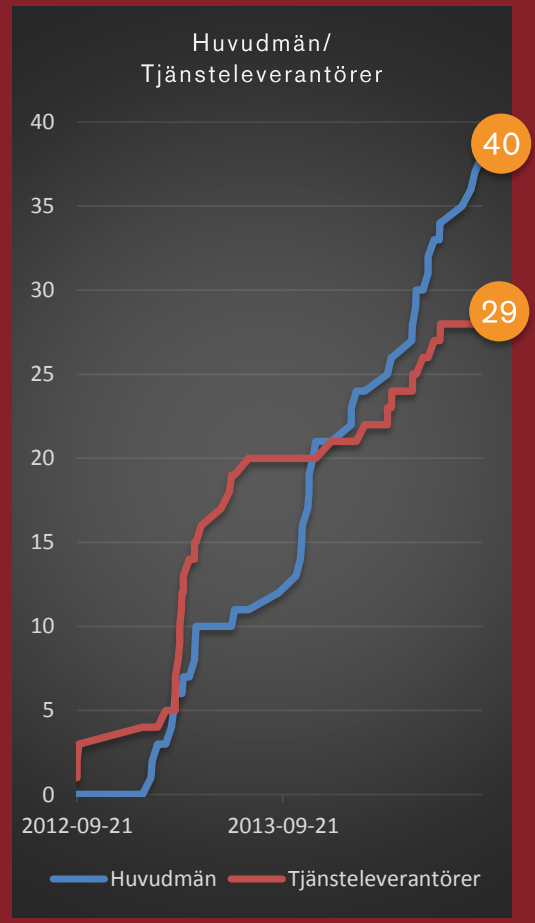
Skolfederation.se

Medlemmar

- Skolhuvudmän
  - skolformer enligt skollagen, allmänt eller privat
  - svensk myndighet som arbetar med skola
  - 40 st medlemmar
- E-tjänsteleverantörer
  - rekommenderad av skolhuvudman
  - 29 st medlemmar

Medlemsutveckling





Skolfederation.se

Passerade milstenar

- Utveckling av system, anvisningstjänst och administrativt gränssnitt
- Etablering av processer och rutiner för medlemshantering, metadatahantering, information, drift och incidenthantering.
- Standardiserade attribut (SIS)
- Testbädd med IdP och SP
- Tilläggstjänsten eduroam
- Signalering av Tillitsnivåer

Skolfederation.se

Uppgifter framför oss

- Hur sänker vi tröskeln för små tjänsteleverantörer med liten budget och begränsad egen IT-kompetens?
- Förprovisionering av användare i e-tjänster (SCIM?)
- Från en drivande roll till en stöttande
- Fortsatt utveckling av system och processer

Skolfederation.se

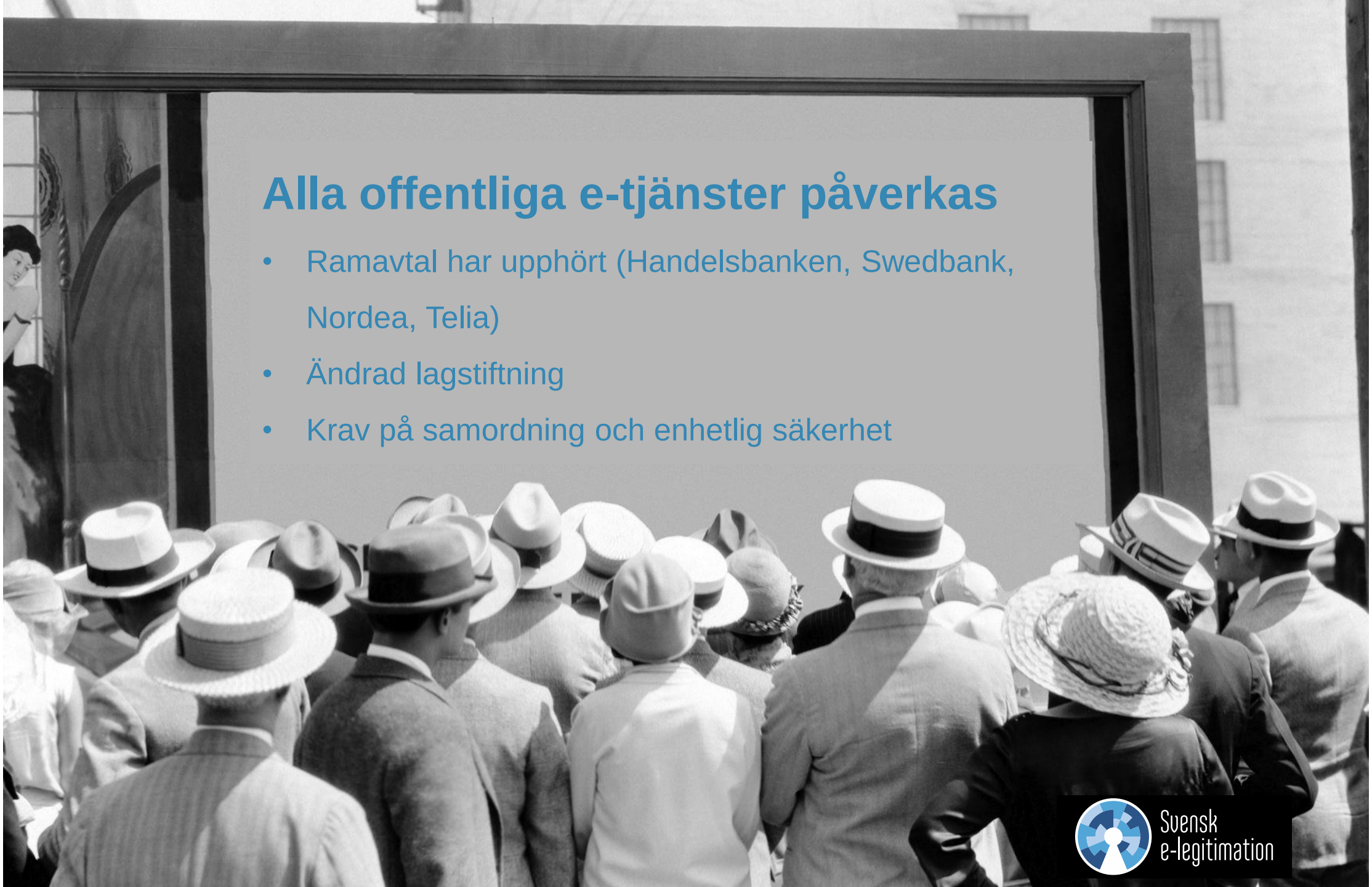
Skolfederation.se

Skolfederation.se

Svensk e-legitimation - en federation på G

Eva Ekenberg, E-legitimationsnämnden


2016 går offentlig sektor över till Svensk e-legitimation
- Är ni redo?
Svensk e-legitimation



Alla offentliga e-tjänster påverkas

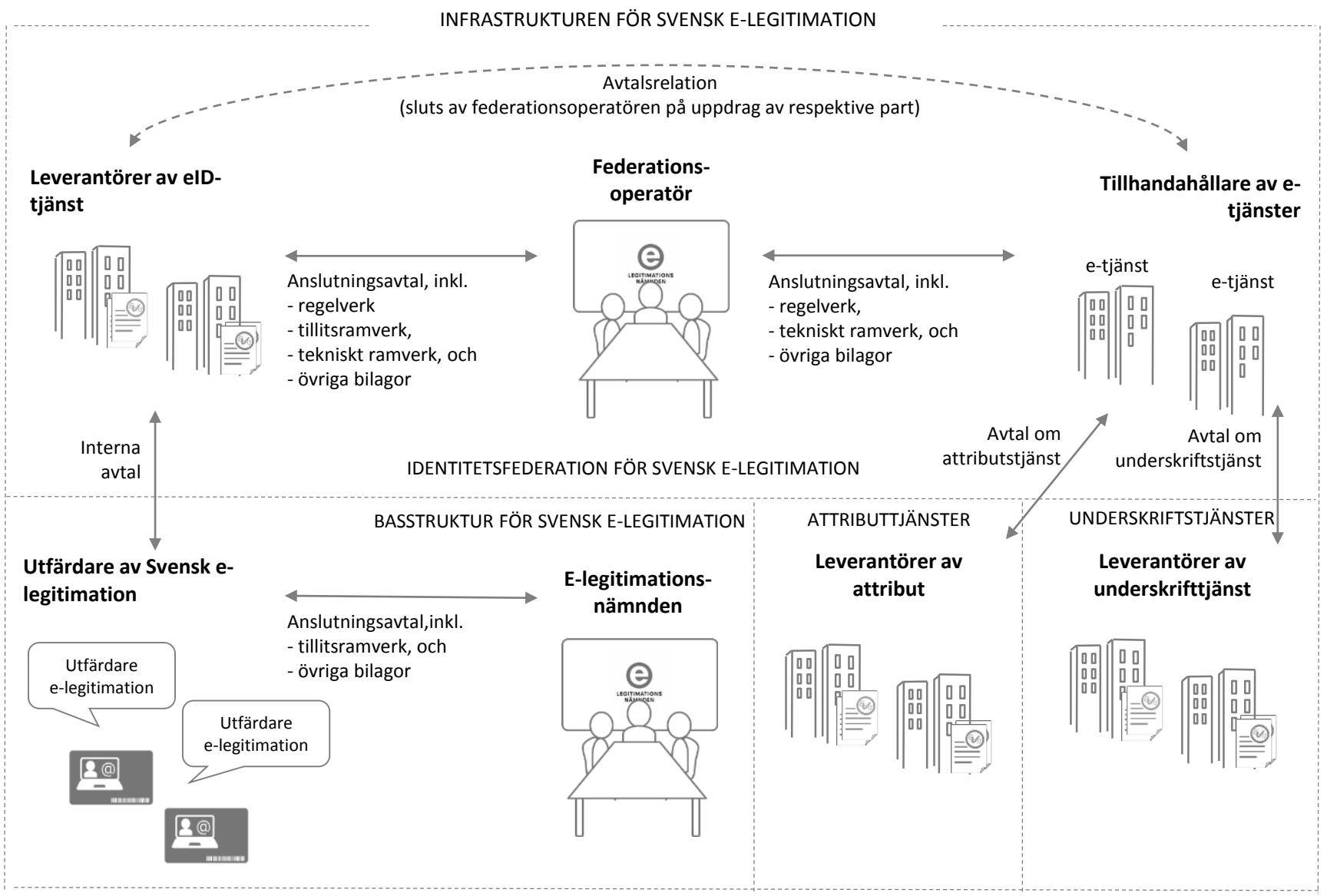
- Ramavtal har upphört (Handelsbanken, Swedbank, Nordea, Telia)
- Ändrad lagstiftning
- Krav på samordning och enhetlig säkerhet

Svensk e-legitimation

Elektronisk identifiering 2016

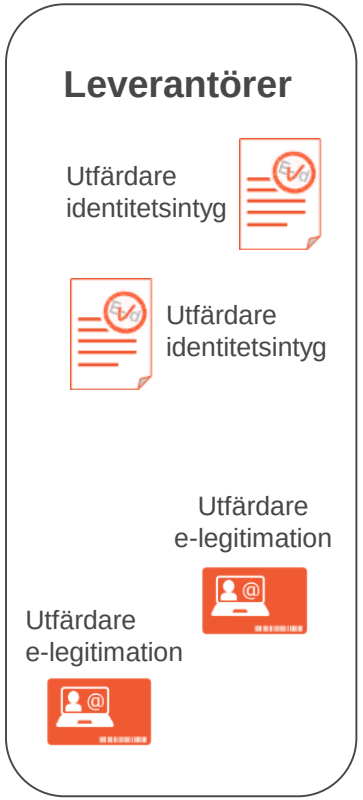
- offentlig sektor

Svensk e-legitimation



Svensk e-legitimation

Granskning och revision



- Ansökan
- Självdeklaration
- Särskild granskningsgrupp
- Kompletteringar
- Stickprov/avgränsad revision

Nyckelord!

- Tillit
- Kostnadseffektivitet
- Balans

Svensk e-legitimation

Klart för anslutning

- Flera har anslutit sig
- Lär mer på www.elegnamnden.se
- Fråga oss - vi berättar gärna mer

Svensk e-legitimation

Eduroam, SWAMID, GÉANT Association och Europeisk interfederering

Valter Nord, SUNET/GÉANT Association

SUNET

SUNET

eduroam, SWAMID och interfederation

SUNET

- Agenda:

- eduroam – en fantastiskt framgångsrik och enorm federation
- SWAMID, interfederationsutmaningar
- Interfederationer och samarbeten inom EU

eduroam

- eduroam

- Ger tillgång till trådlöst internet
- Målgrupp utbildningssektorn
- Startade ca 2003
- Efterfrågan fanns i Sverige, ca 2004/2005 fanns liknande lösning
- 2006 började vi rulla ut eduroam

eduroam

- eduroam – lite siffror
- Finns på fler än 10.000 ställen i Europa + resten av världen.
- ”One purpose” federation, att få tillgång till internet
- Begränsat med val/alternativ
- Medverkande parter följer en gemensam standard
- Enkelt att motivera investering

eduroam

- I Sverige är idag alla lärosäten inom högre utbildning anslutna
- Grundskolor och gymnasieskolor ansluter sig genom skolfederationen
- Medverkande parter följer en gemensam standard

- Interfederation som fungerar!

SWAMID

- Gammal är äldst..
- Alla lärosäten plus relevanta myndigheter uppkopplade, ca 50 IdP
- Fokus på att höja förtroendenivån
- Målet ”bekräftad” användare för merparten (AL2)
- Lång väg dit…

SWAMID

- Lärdomar:

- Keep it simple
- En ”killer application” hjälper
- Vi bryter ny mark – det behövs stöd
- Federativa aktiviteter är sällan högst upp på agendan
- Använd morot mer än piska

SWAMID

- Fortsatta lärdomar och nästa steg:

- Jobba ännu mer med information
- Skapa tydliga informationskanaler
- Bygg upp ett aktivt community
- Under 2015 kommer SWAMID AL1 att implementeras fullt ut

SWAMID och interfederation

- Mer information än eduroam!
- Fördras Förnamn, Efternamn eller Efternamn, Förnamn?
- Hanteras något annorlunda i olika federationer inom Europa.
- Teknisk kompatibilitet fastställd genom att vi använder samma SAML-profil (SAML2int)

SWAMID och interfederation

- Två lösningar
- Proxies mellan varje land som översätter -> samlar på sig ”ALL” information om individen
- De tjänster som exponeras internationellt hanterar båda formaten!

SWAMID och interfederation

- Att harmonisera på internationell nivå är en trög process.
- Någon som är beredd att definiera student i hela Europa?
- Lokal anpassning behövs beroende på kultur, historik etc

Nationella forum

- .SE – Skolfederationen
- SUNET – SAML-admins
- SUNET – eduroam-admins
- E-legnämnden – EID2.0
- Internetdagarna

Internationella forum

- REFEDS
- ”Task forces” inom TERENA (www.terena.org)
- Kantara
- ISOC
- IETF

SUNET

Tack för att ni lyssnat!

Frågor?

Valter Nordh
valter@sunet.se

www.swamid.se - www.sunet.se

Vilken påverkan får eIDAS - Electronic Identification and Signature, på Sveriges infrastruktur?

Håkan Persson, Arbetsförmedlingen

eIDAS
EU's förordning om elektronisk identifiering

2014-11-25

Håkan Persson

Arbetsförmedlingen

Arbetsförmedlingen

eIDAS förordningen

- *EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG*
  - En förordning gäller, till skillnad från ett direktiv, över svensk lag
- Det mesta i förordningen skall tillämpas fr.o.m. 2016-07-01
- Alla detaljer i förordningen är dock inte helt klara ännu och fastställs genom sk. ”genomförandeakter” det närmaste året
- Förordningen: http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32014R0910

Arbetsförmedlingen

Artikel 6 - gäller fr.o.m. 2018-09-18

- *När det enligt nationell rätt eller enligt nationella administrativa förfaranden krävs en elektronisk identifiering där medel för elektronisk identifiering och autentisering används för att få åtkomst till en nättjänst **som tillhandahålls av ett offentligt organ** i en medlemsstat, **ska** de medel för elektronisk identifiering som **utfärdats i en annan** medlemsstat **erkännas** i den första medlemsstaten för gränsöverskridande autentisering för den tjänsten via internet, förutsatt att*
  - *a) medlet för elektronisk identifiering är utfärdat inom ramen för ett system för elektronisk identifiering som **ingår i den förteckning** som offentliggjorts av kommissionen enligt artikel 9,*
  - *b) tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög som eller högre än den tillitsnivå som det berörda offentliga organet kräver för åtkomst till denna nättjänst i den första medlemsstaten, förutsatt att tillitsnivån för detta medel för elektronisk identifiering motsvarar **tillitsnivån väsentlig eller hög**,*
  - *c) det offentliga organet i fråga **använder** tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten.*
- *Ett sådant erkännande ska ske **senast tolv månader** efter det att kommissionen offentliggör den förteckning som avses i led a i första stycket.*

Arbetsförmedlingen

Tillitsnivåer (Artikel 8)

- Förordningen fastställer tre tillitsnivåer för anmälda system
  - *I ett system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 ska tillitsnivåerna **låg**, **väsentlig** och/eller **hög** specificeras för medel för elektronisk identifiering som har utfärdats inom det systemet*.
- Arbetet med att specificera tillitsnivåerna pågår fortfarande och skall beslutas i en genomförandeakt
- Tillitsnivåerna beskrivs i ”värdeladdade ord” som ”*assumed to be in possession of*” och “*verified to be in possession of*”
  - ”Outcome based” i stället för ”Normative”
  - Kompletteras med ett “Guidance document” (Vägledning)
- Mycket av det ömsesidiga förtroendet för varandras system kommer att ske via olika samarbetsgrupper

Arbetsförmedlingen

Betrodda tjänster som också regleras i förordningen

- Utfärdande av certifikat för elektroniska underskrifter och stämplar
- Validering av underskrifter och stämplar
- Bevarande av underskrifter och stämplar
- Tidsstämpling
- Elektronisk rekommenderad leverans av dokument
- Certifikat för autentisering av webbplatser

Arbetsförmedlingen

EU Trust Mark (Artikel 22)

Arbetsförmedlingen

På väg mot en inre elektronisk marknad?

Arbetsförmedlingen

Arbetet går vidare

hakan.z.persson@arbetsformedlingen.se

Svenskt federationsforum

Pause

Åter kl 14.00

Ladok3, ett nationellt studieadministrativt system utan användarkonton

Fredrik Åslund, Umeå universitet

Ladok3, ett nationellt studieadministrativt system utan användarkonton

Fredrik Åslund, Ladok3-projektet, Umeå universitet

Svenskt federationsforum

2014-11-25

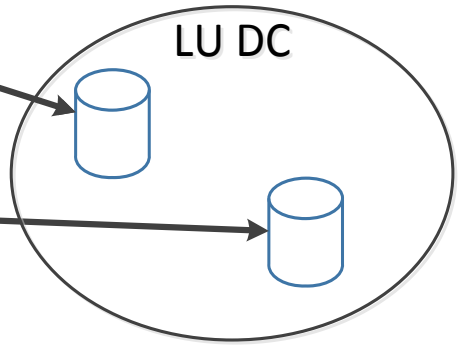
Ladok

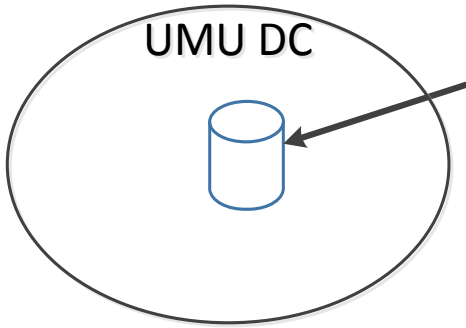
Innehåll

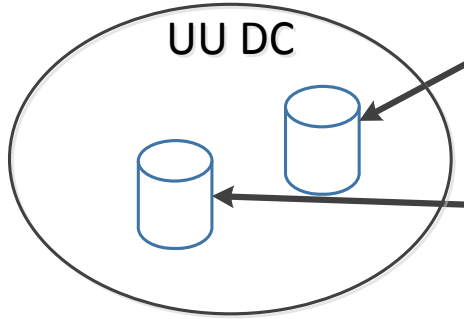
- Det här är Ladok
- Nuvarande Ladok
- Nya Ladok
- Inloggning
- Behörigheter
- Testmiljöer

Ladok

- Nationellt system för studieadministration inom högre utbildning
- Utbildningar, registrering, resultat, intyg, …
- Ägs av lärosätena tillsammans
- Egna instanser, tre driftcentraler

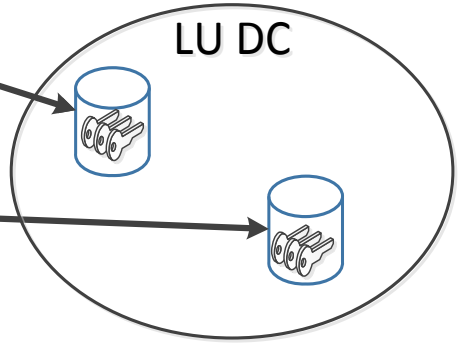


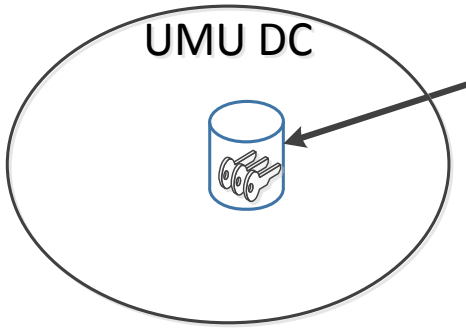


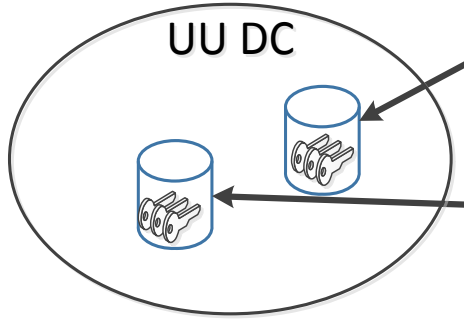


Användare i Ladok

- Totalt runt 5000 användare för alla lärosäten
- Användardatabasen ligger i Ladok







Ladok3-projektet

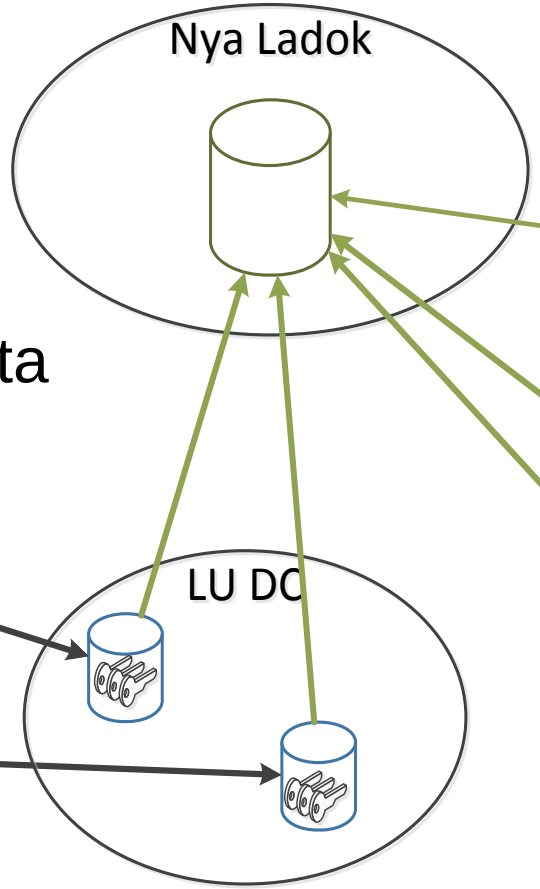
- 2009 beslutades att ett nytt Ladok-system skulle byggas

- Åldrande teknisk plattform
- Höga kostnader för förändringar
- Ökande underhållskostnader
- Låg informationskvalitet
- Bristande stöd för integrationer

- Ladok3-projektet ska bygga nästa generation av studieadministrativt systemstöd för universitet och högskolor i Sverige

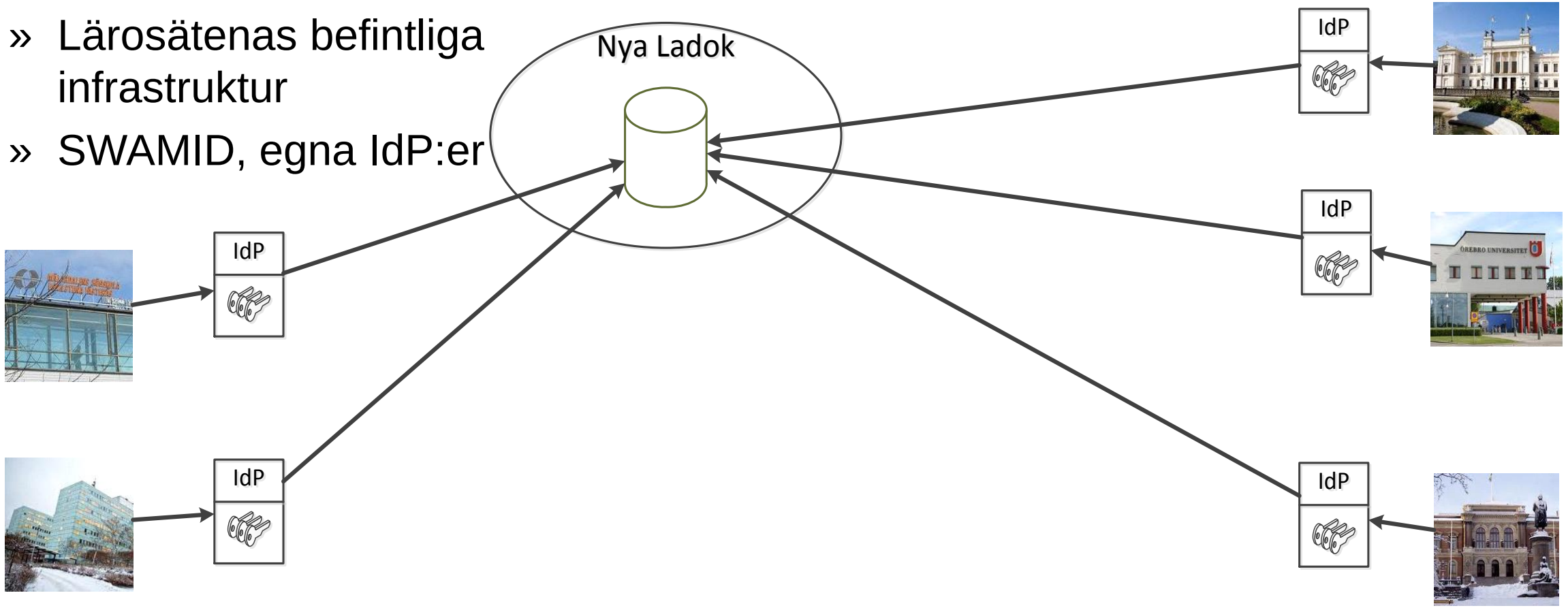
Migrering från gamla till nya Ladok

- Ett centralt system
- Data konverteras in i nya Ladok
- Lärosätena äger fortfarande sin data



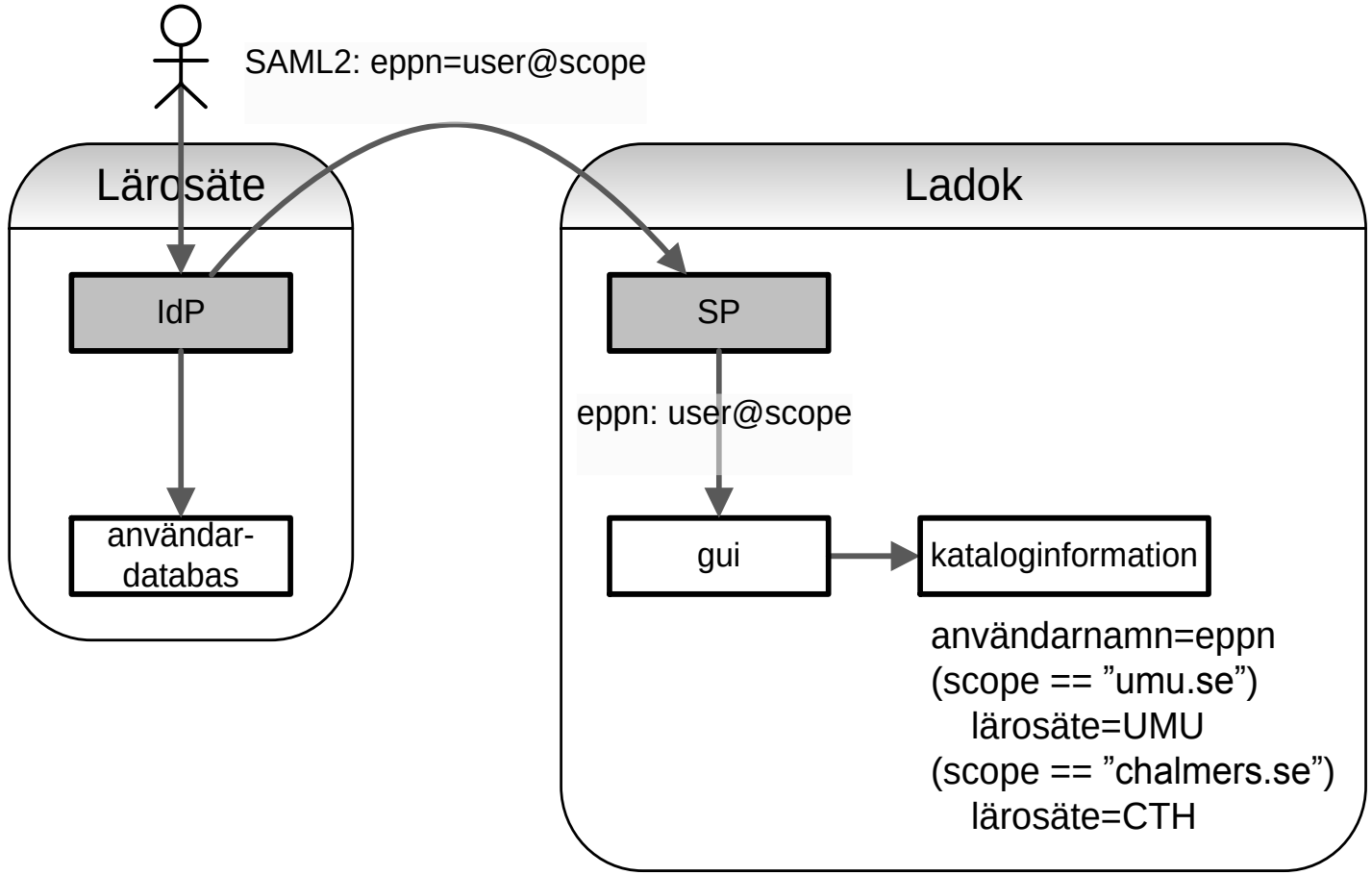
Inloggning i nya Ladok

- Lärosätenas befintliga infrastruktur
- SWAMID, egna IdP:er



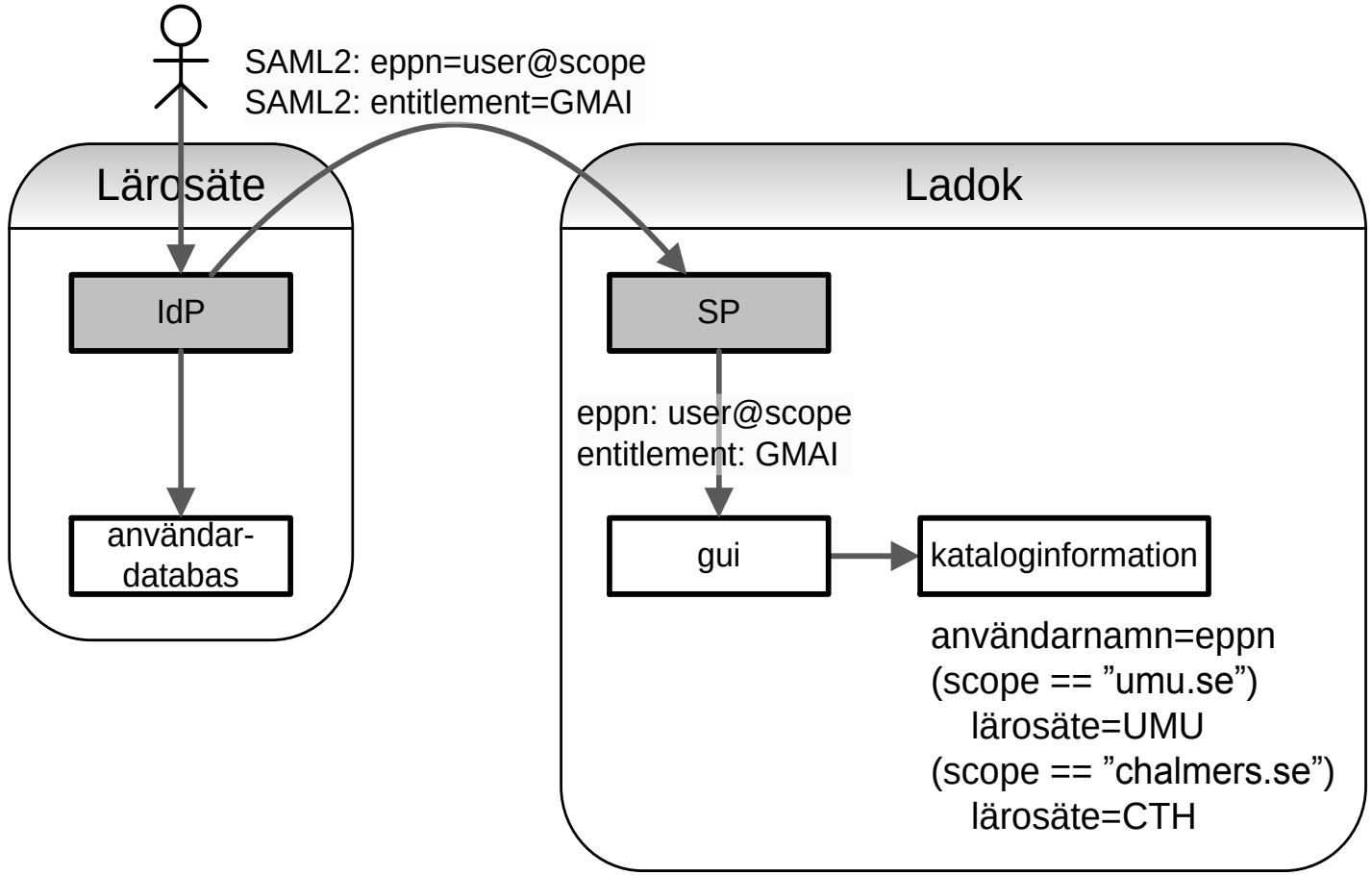
Första inloggningen

- En identitet skapas
- eduPersonPrincipalName används som nyckel
- Scope mappas till lärosäte
- Behörigheter kan beställas som godkänns av en lokal administratör
- Behörigheter lagras i kataloginformation



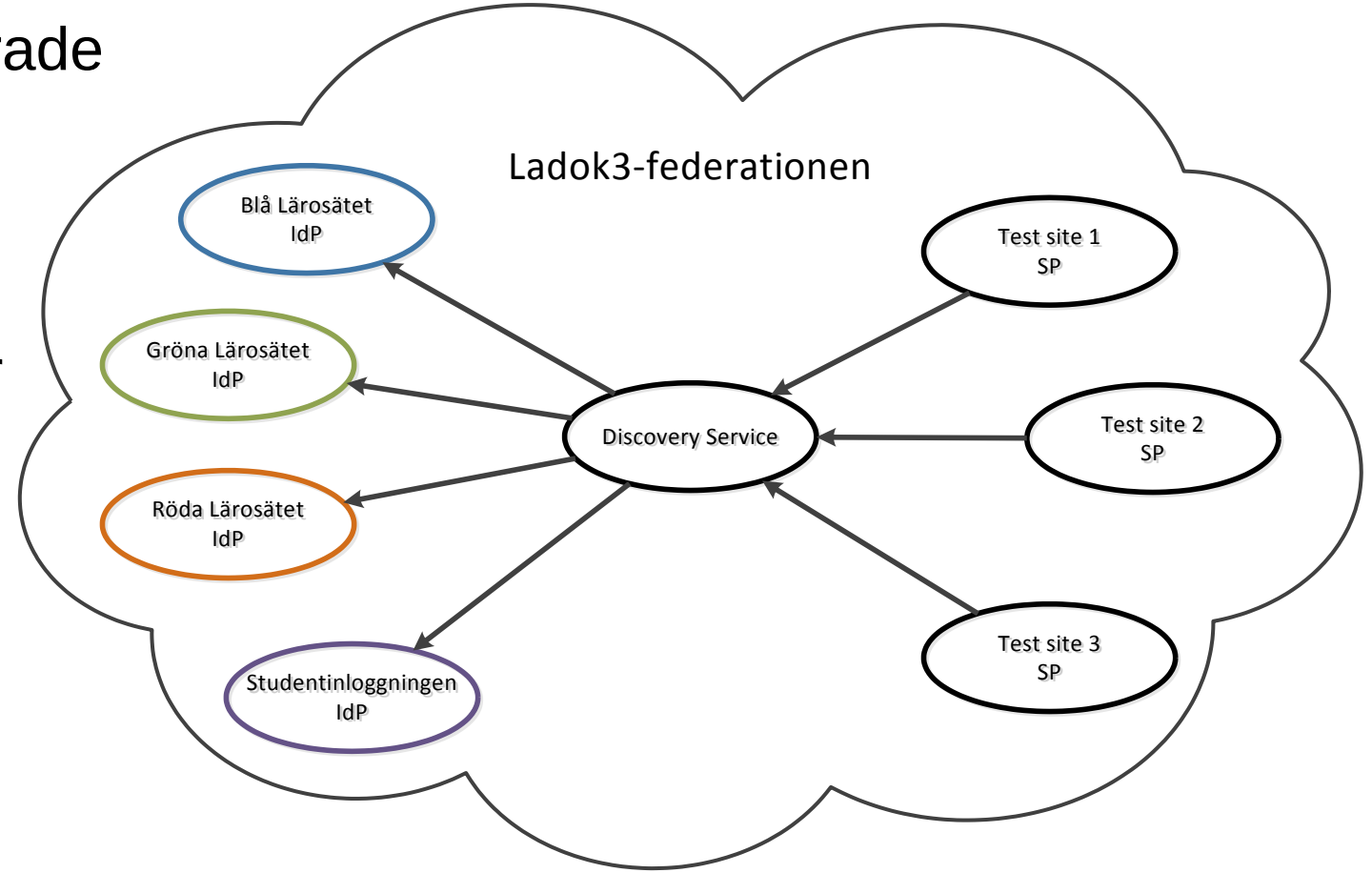
Behörigheter via SAML (entitlements)

- IdP:er kan skicka behörigheter via entitlements
- Möjliggör lokal hantering av behörigheter via egna användarkataloger



Testmiljöer

- Egna IdP:er med fördefinierade användare
- Egen Discovery Service för att välja IdP
- Egen federation med IdP:er SP:s och en DS



Frågor?

» Frågor?

» Mer information
- www.ladok.se
- fredrik.aslund@umu.se

Federationsanpassning av Ineras Säkerhetstjänster

Björn Skeppner, Inera

Federationsanpassning av Inera:s Säkerhetstjänster

(Vad är nyttan med att Säkerhetstjänsternas IdP och vårdens tjänster ansluter sig till Sambi?)

2014-11-25

Björn Skeppner, IT-arkitekt, Inera

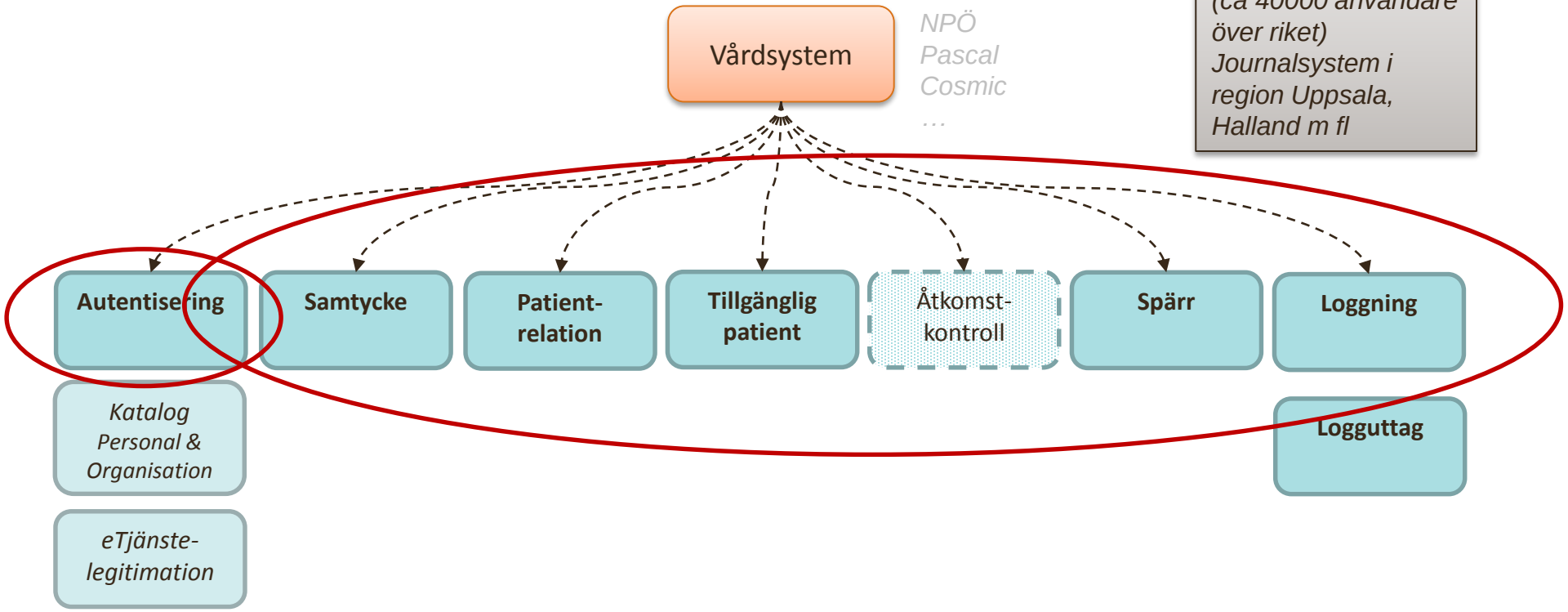
Kort bakgrund

- CeHis handlingsplan:
  *90% av medarbetarna kan år 2016 nå sina professionella verksamhetssystem med **en** samordnad, enkel och säker inloggning (SSO)*

- Idag användarnamn & lösenord!
- För det mesta Client Server-baserade (rika klienter).
  Det går trögt att avveckla Windows XP ☹

Säkerhetstjänster för eHälsa

NPÖ (alla landsting, ca 70 kommuner)
Pascal
(ca 40000 användare över riket)
Journalsystem i region Uppsala, Halland m fl



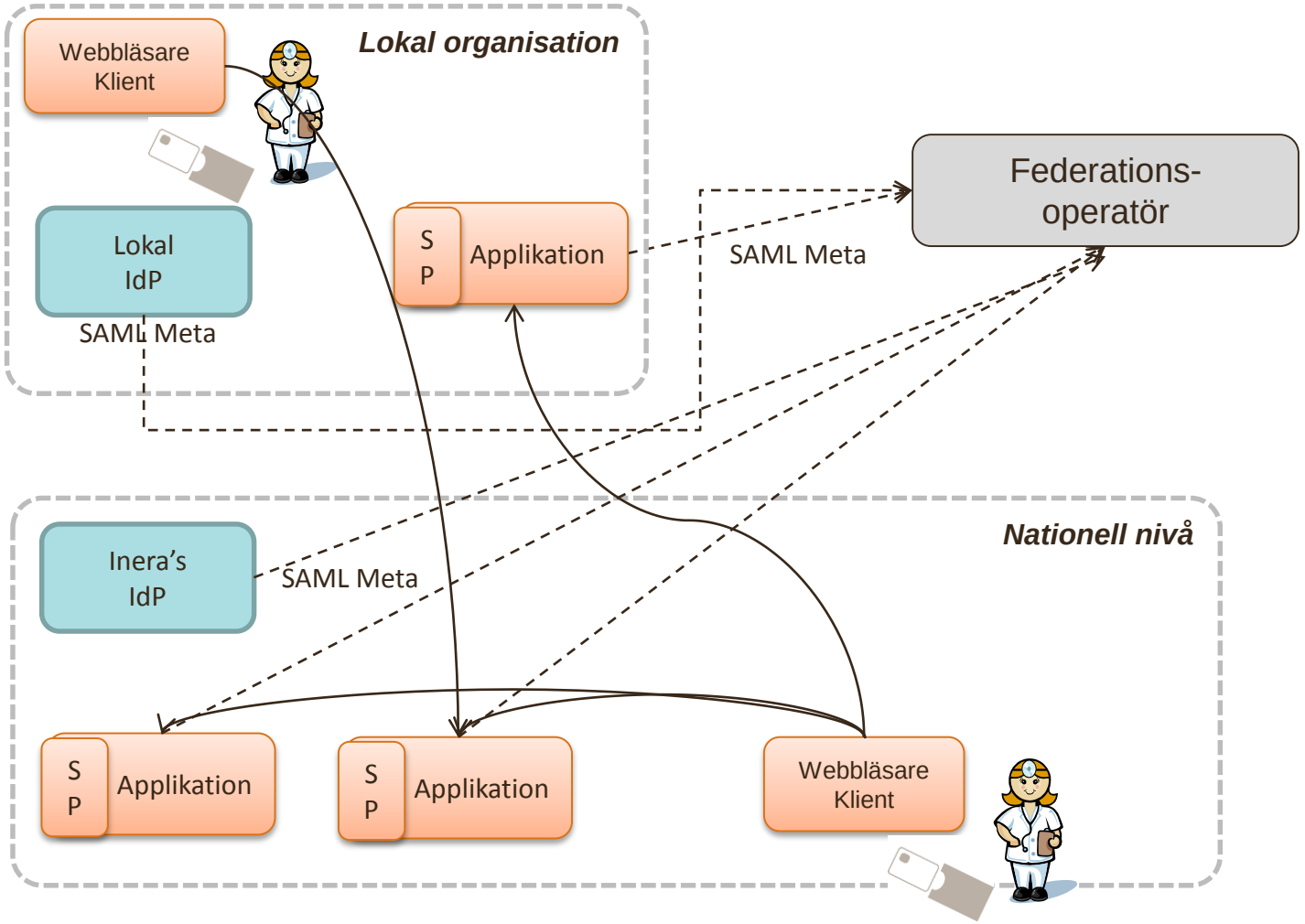
Identifiering

Sätt spärr

Ge samtycke

Kontrollera loggar

Autentiseringstjänst 2.x – *med SAMBI*



Fördelar med SAMBI

- Gemensamt regelverk
- Riktig Single Sign On (SSO)
- Hög säkerhet
- Mindre administration (än bilaterala överenskommelser)

Nackdelar med SAMBI

- Kan vara hög tröskel för en del verksamheter att uppfylla regelverket
- Kräver mer samsyn kring attributshantering

Pågående SAMBI-aktiviteter (Inera)

- Säkerhetstjänster har samtestat med Svensk e-identitet:s IdP och SP
- Att få med Inera:s tjänster (Pascal/NOD etc) i SAMBI
- Upprätta en attributförvaltning för SAMBI
- Att fundera mer kring SLO!

Noterbart…

- eHälsomyndigheten avser att nyttja SAMBI vilket i så fall kräver att de verksamheter som vill komma åt tjänsterna hos eHälsomyndigheten (NOD, läkemedelsförteckningen etc) också behöver ha sina e-tjänster anslutna till SAMBI!

Tack för mej!

(hoppas jag höll tiden?

eHälsomyndighetens och Ineras POC för web services

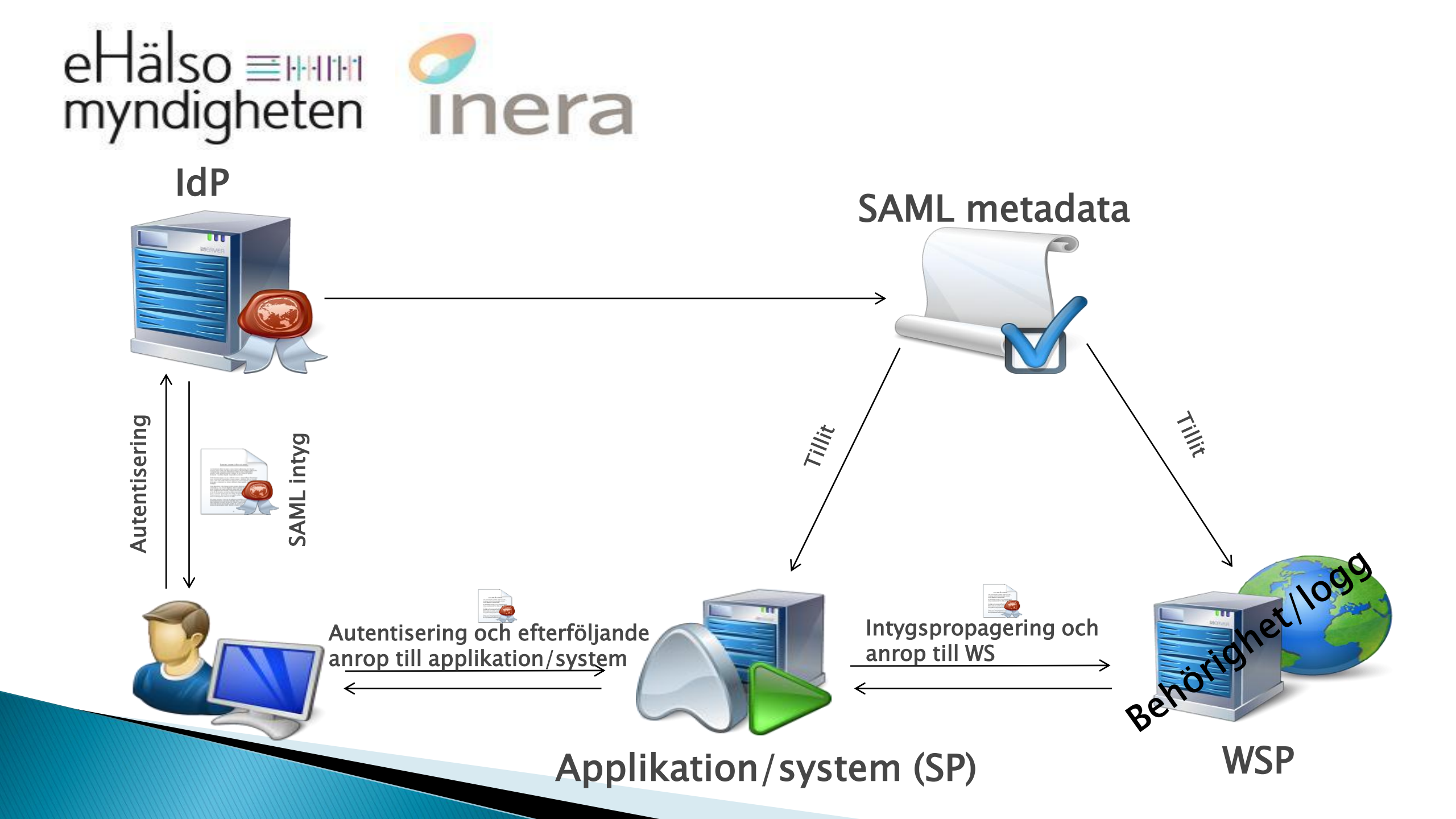
Conny Balazs, för eHälsomyndigheten

Intygspropagering
Vad och varför?

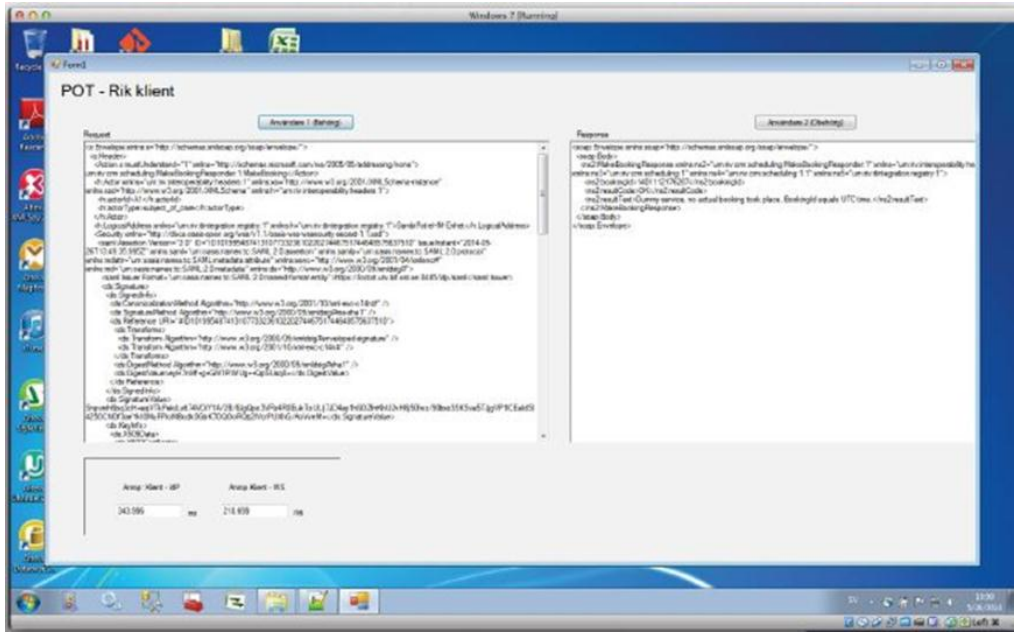
eHälsomyndigheten inera

Projektets syfte

- Förbättra och effektivisera integration mellan olika organisationer i webservicemiljöer
- Dra nytta av den nationella infrastruktur som deltagande parter önskar samverka med hjälp av
- Ge möjlighet till förstärkt nivå av tillit mellan organisationer

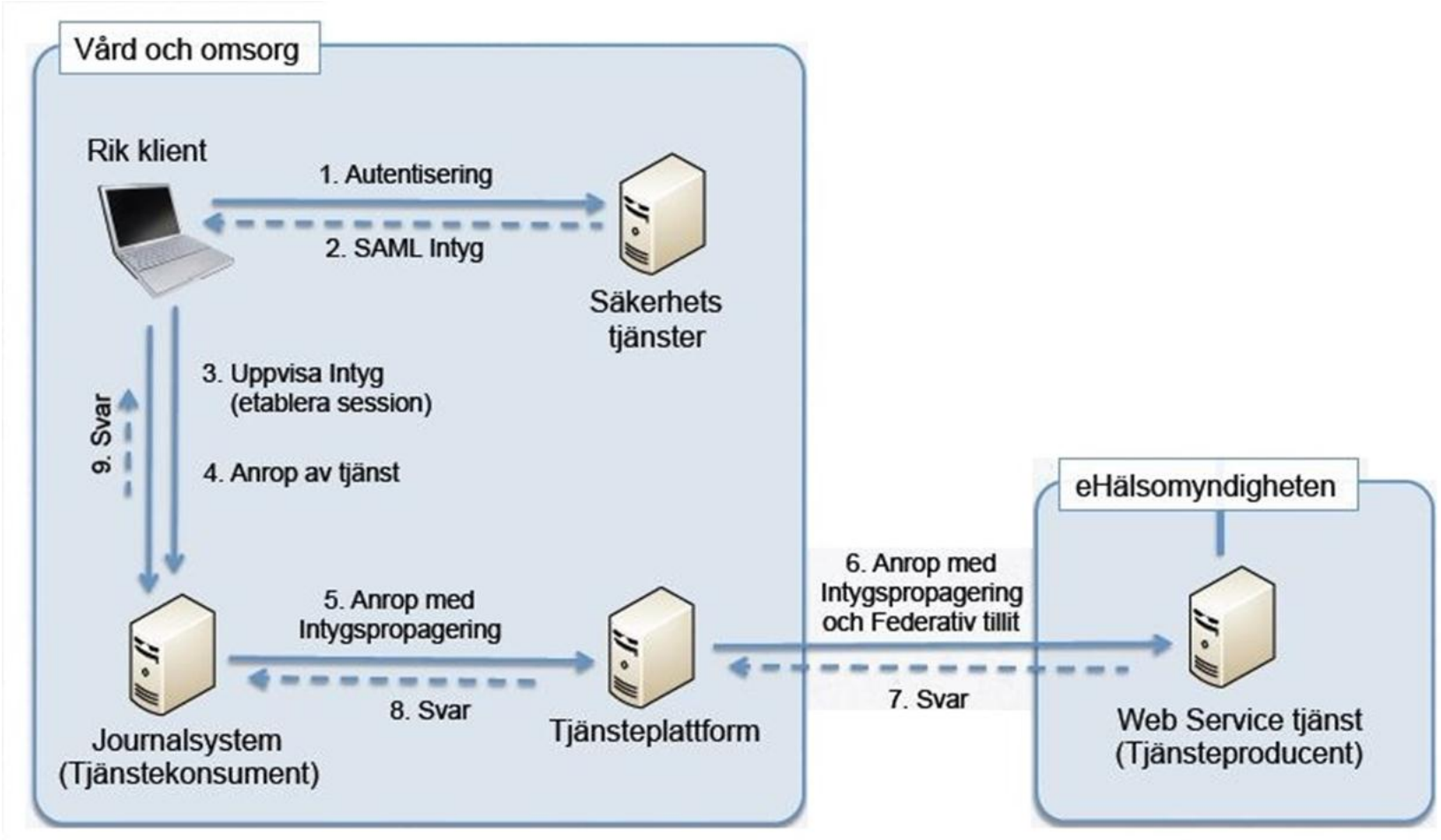

IdP
SAML metadata
Tillit
Tillit
Autentisering
SAML intyg
Autentisering och efterföljande
anrop till applikation/system
Intygspropagering och
anrop till WS
Behörighet/logg
Applikation/system (SP)
WSP

- Projektet levererade en komplett referenstillämpning
  - Kördes i projektet över nationell integrationsplattform



eHälso myndigheten

inera



Projektets resultat

- Kvalitetssäkrade och testade specifikationer för användningsfall
- Vidare arbete med gemensam roadmap för införande
- Öppenhet gällande specifikationer och leveranser

För mer information

- Stefan Larsson, eHälsomyndigheten
  - stefan.larsson@ehalsomyndigheten.se
- Björn Skeppner, Inera
  - bjorn.skeppner@inera.se
- Conny Balazs, Certezza
  - conny.balazs@certezza.net

eHälso myndigheten

inera

En Testspecifikation för Sambis test- och demonstrationsbädd

Ulrika Ahlgren, .SE

Sambi
Samverkan
för säkrare
e-hälsa

En testspecifikation för Sambi’s test- och demonstrationsbädd

Ulrika Ahlgren
.se

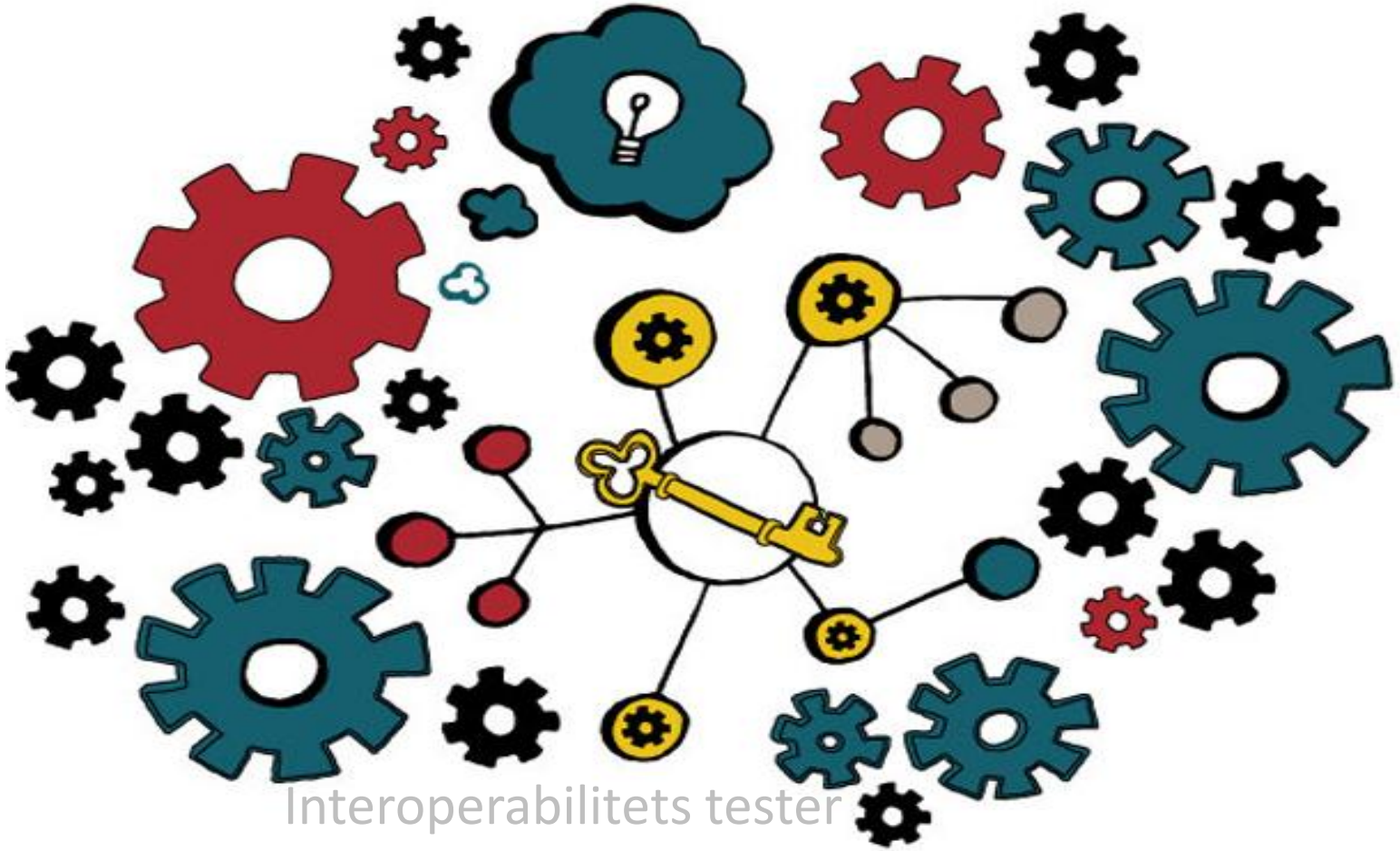
Sambi
Samverkan
för säkrare
e-hälsa

- Vad det är vi gör
- Varför vi gör det här
- Status

Sambi
Samverkan
för säkrare
e-hälsa

Vad är det som testas?

Användare



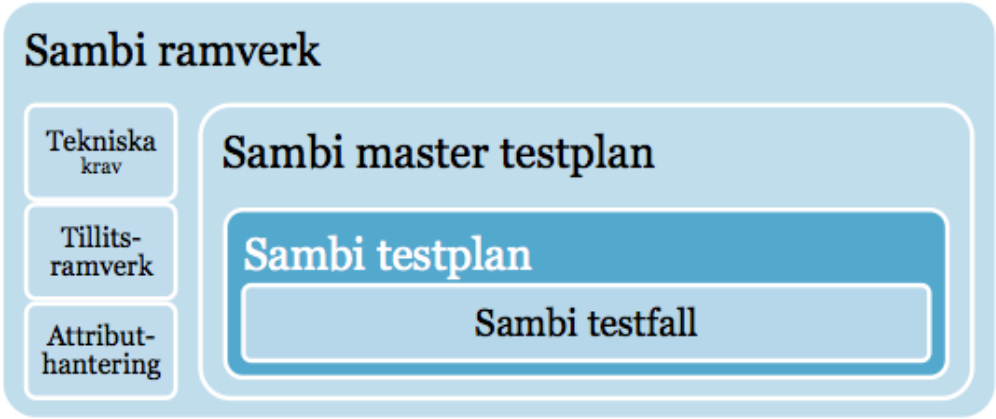
Interoperabilitets tester

Tjänst/er

Sambi
Samverkan
för säkrare
e-hälsa

Test dokument

- Master testplan
  - Övergripande beskrivning av test miljö, ordlistor förklaringar m.m.
- Testplan
  - Testkrav
  - Mappning mellan testkrav och tester.
- Testfall
  - Detaljbeskrivning över de olika testerna.



- Bygger på IEEE 829-2008
- Nyckelord från RFC 2119

Sambi
Samverkan
för säkrare
e-hälsa

Testområden

- Hantering av Metadata
- Identifieringsbegäran
- Identifieringssvar
- Attribut
- Byte av tillitsnivå (LoA)
- Logout och Single LogOut (SLO)

Sambi
Samverkan
för säkrare
e-hälsa

Sambi Test — Aktiva

- Inera (CGI)
- MobilityGuard
- Nexus
- Stockholms Läns Landsting (SLL)
- Stockholms stad
- Svensk e-identitet
- Tieto

- eHälsomyndigheten
- Migrationsverket
- Pulsen Combine

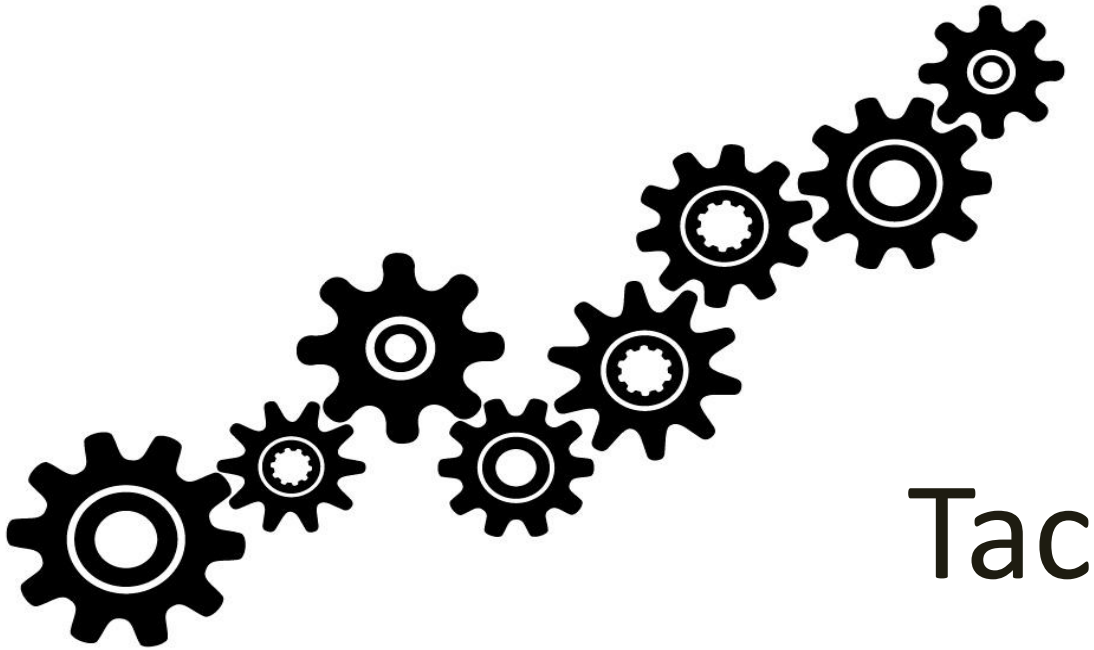
Sambi
Samverkan
för säkrare
e-hälsa

https://www.sambi.se

Sambi
Samverkan
för säkrare
e-hälsa

- Varför gör vi det här?
- Vad är det vi gör
- Status

Sambi
Samverkan
för säkrare
e-hälsa



Tack!

Appar och federationer

Thomas Nilsson och Conny Balazs, Certezza

CERTEZZA

sju korta minuter om… appar och federationer

Conny Balazs & Thomas Nilsson
conny@certezza.net & thomas@certezza.net

CERTEZZA

Appar och federationer?

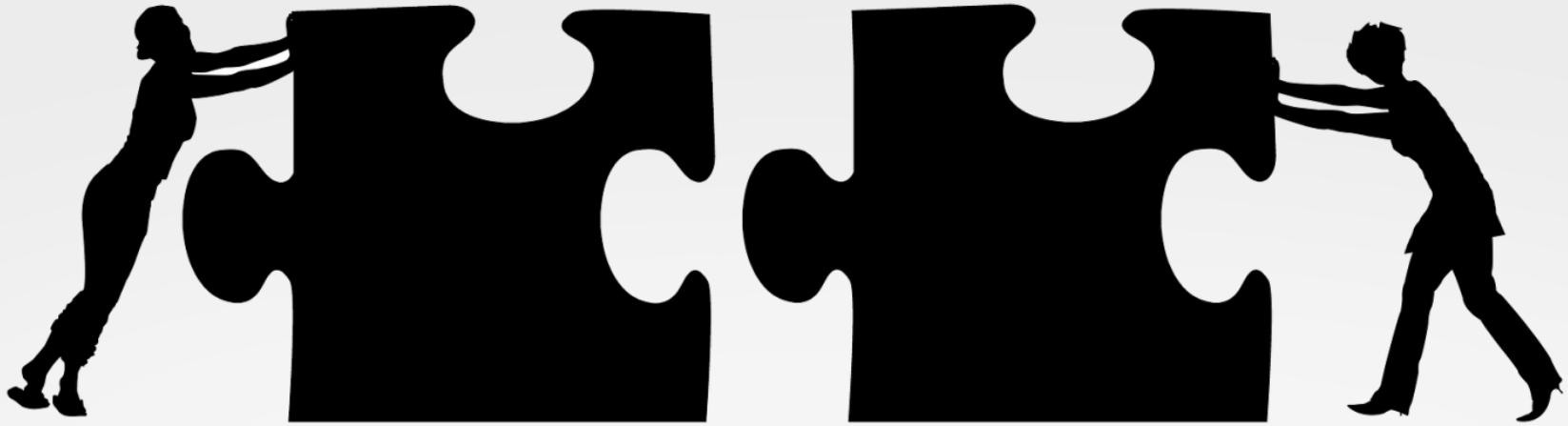
CERTEZZA

Olika typer av appar

- Native app
  - "rik" klient på mobil plattform
- Hybrid app
  - native app med integrerat webbkit
- HTML5 single page app
  - webkit som serveras innehåll från WS-API:er
- HTML5 multi page app
  - webkit som serveras innehåll från webbapplikation och/eller WS-API:er

CERTEZZA

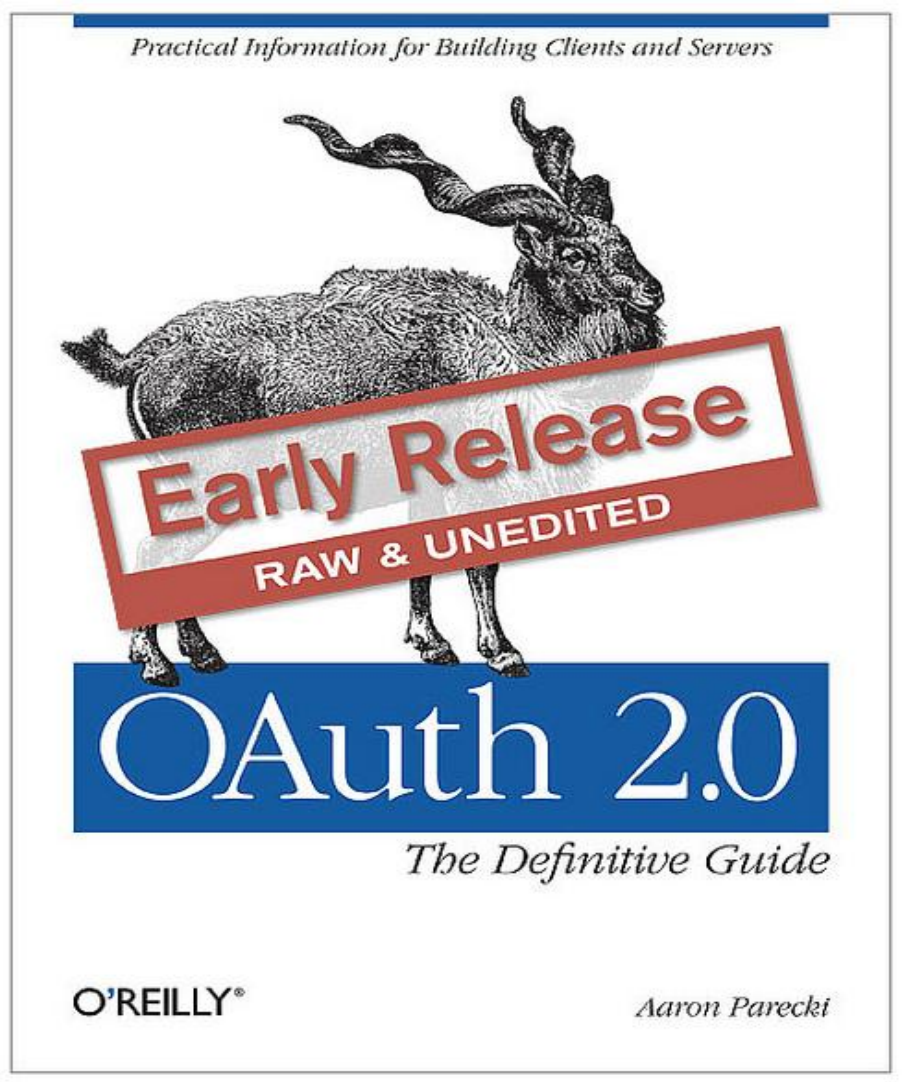
Vad fattar appar?



Välj gärna ett modernt och smakfullt alternativ!

CERTEZZA

And the winner is…



CERTEZZA

Äktenskapet SAMLv2 och OAuth2.0

- SAML och OAuth kompletterar varandra ovanligt bra!
- SAML – för att nyttja federerade identiteter, egenskaper och autentisering
- OAuth – för att auktorisera en klient efter utförd autentisering
  - Ger en app rätt att exekvera i en användares *user context*
  - Möjliggör för icke webbappar att interagera med en federation på ett modernt sätt

CERTEZZA

Nästan bara fördelar…

- OAuth har bästa tänkbara stöd i utvecklingsmiljöer och kodbibliotek
- Standard WEBSSO i dialogen med federationen
- Användaren får självklart SSO
  - mellan flera appar om så önskas
  - även SLO om så önskas
- Ingen låsning till specifika autentiseringsmetoder
  - Sköts i vanlig ordning på IdP-sidan
- Sist men inte minst - öppna standarder som är plattforms- och leverantörsoberoende!

CERTEZZA

Men, välj OAuth-flöde med omsorg!

- Oauth-flows motsvarar ungefär SAML-profiler
- Beskriver interaktioner mellan:
  - Användare
  - Klient
  - Authorization endpoint
  - Resurs
- Här kan det bli tankevurpor…

CERTEZZA

Vi berättar mer på…
www.sakerhetsdagen.se

Erfarenhetsutbyte – Blixttal

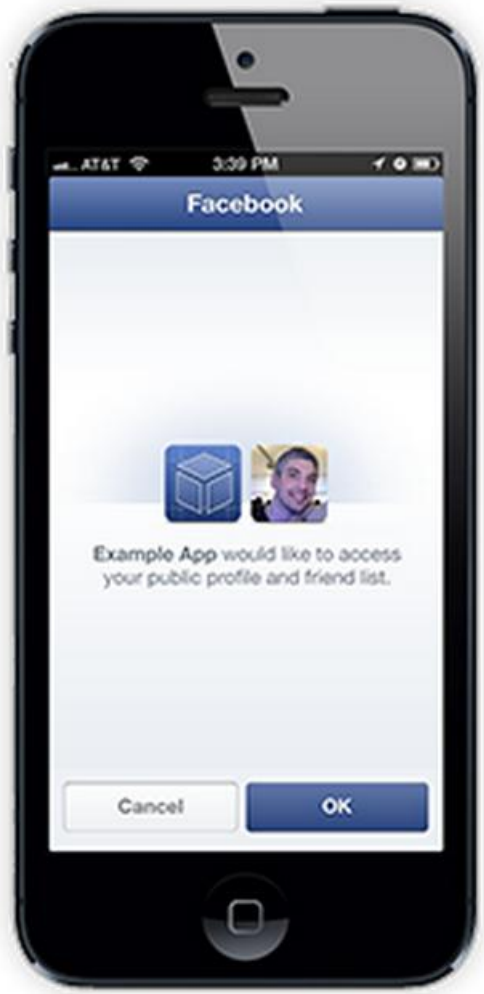
Säker inloggning och federerade identiteter i appar

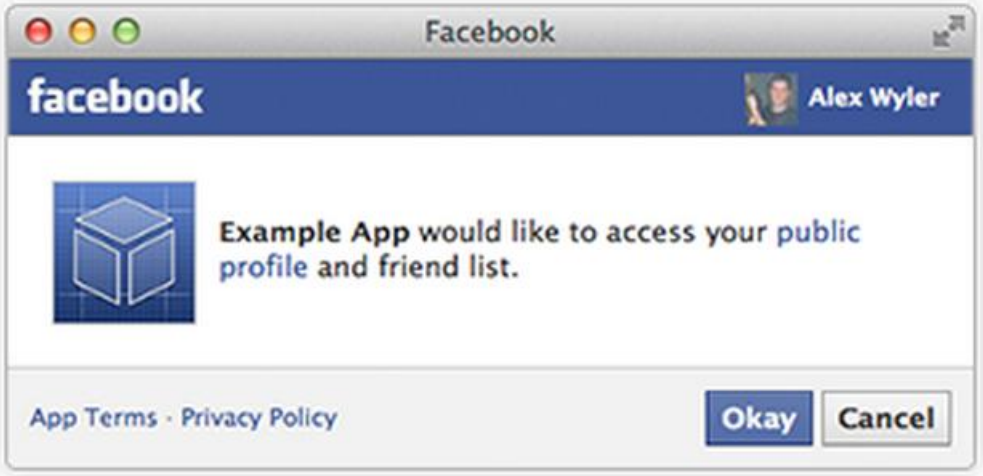
Erik Wahlström, neXus


nexus
your access to success


MPH
km/h

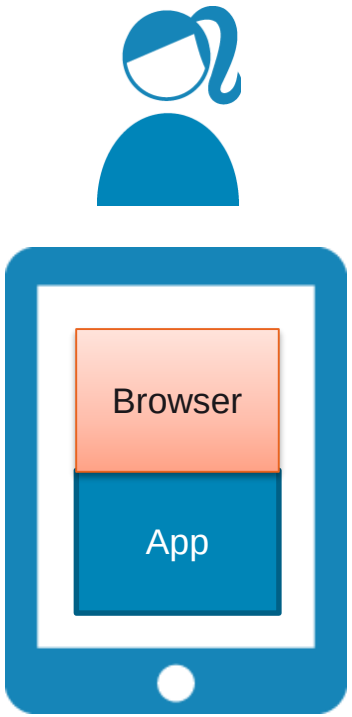

OAUTH
2
OAUTH


AT&T
3:39 PM
Facebook
Example App would like to access your public profile and friend list.
Cancel
OK

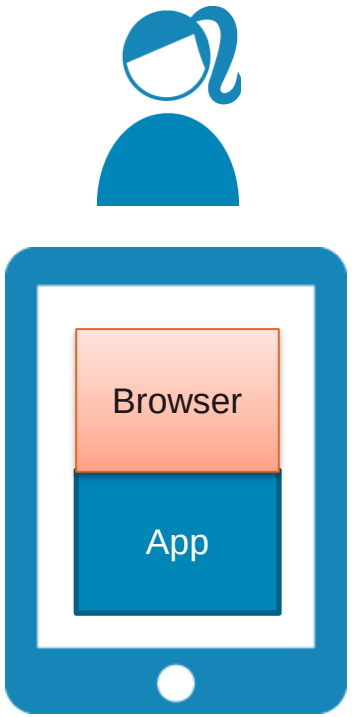

Facebook
facebook
Alex Wyler
Example App would like to access your public profile and friend list.
App Terms · Privacy Policy
Okay
Cancel


Facebook
"Friend Smash!" would like to access your basic profile info and list of friends.
Don't Allow
OK

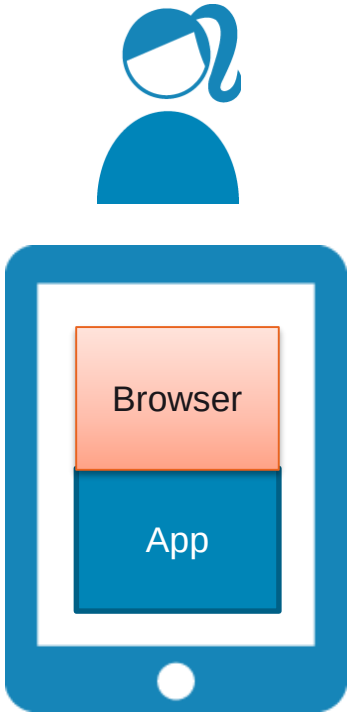

Facebook
Foursquare would like to access your public profile and friend list.
Cancel
OK


Browser
App


OAUTH
2
OAUTH

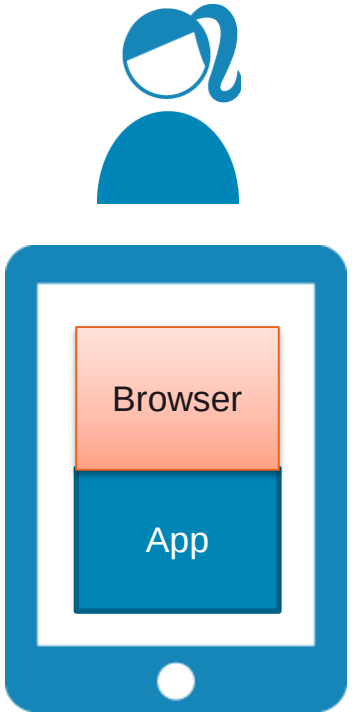

Browser
App


****
OAUTH
2
OAUTH

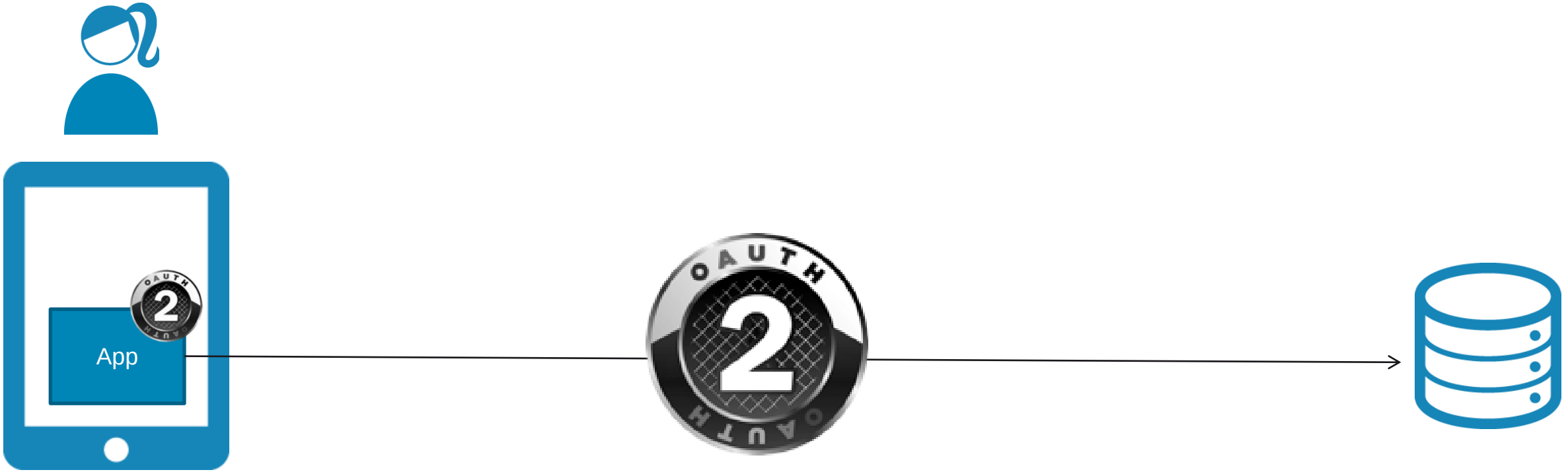

Browser
App


****
OAUTH
2
OAUTH


Skolfederation.se


Browser
App


****
OAUTH
2
OAUTH


App

Erik Wahlström
Product Strategist
11/27/2014


```
gapi.auth.authorize(
        {
            client_id: clientId,
            scope: scopes,
            immediate: false
        },
        handleAuthResult);
```

”izj9832jicj8sjxm3”

Erik Wahlström
Product Strategist

OAuth2 är framtiden

Federera mera.

Låt världen förändras.

Fokusera på appen.

Erik Wahlström

erik.wahlstrom@nexusgroup.com

@erik_wahlstrom

Anslutning av appar till federationer

Jörgen Hellgren, Svensk e-identitet AB

Svensk e-identitet

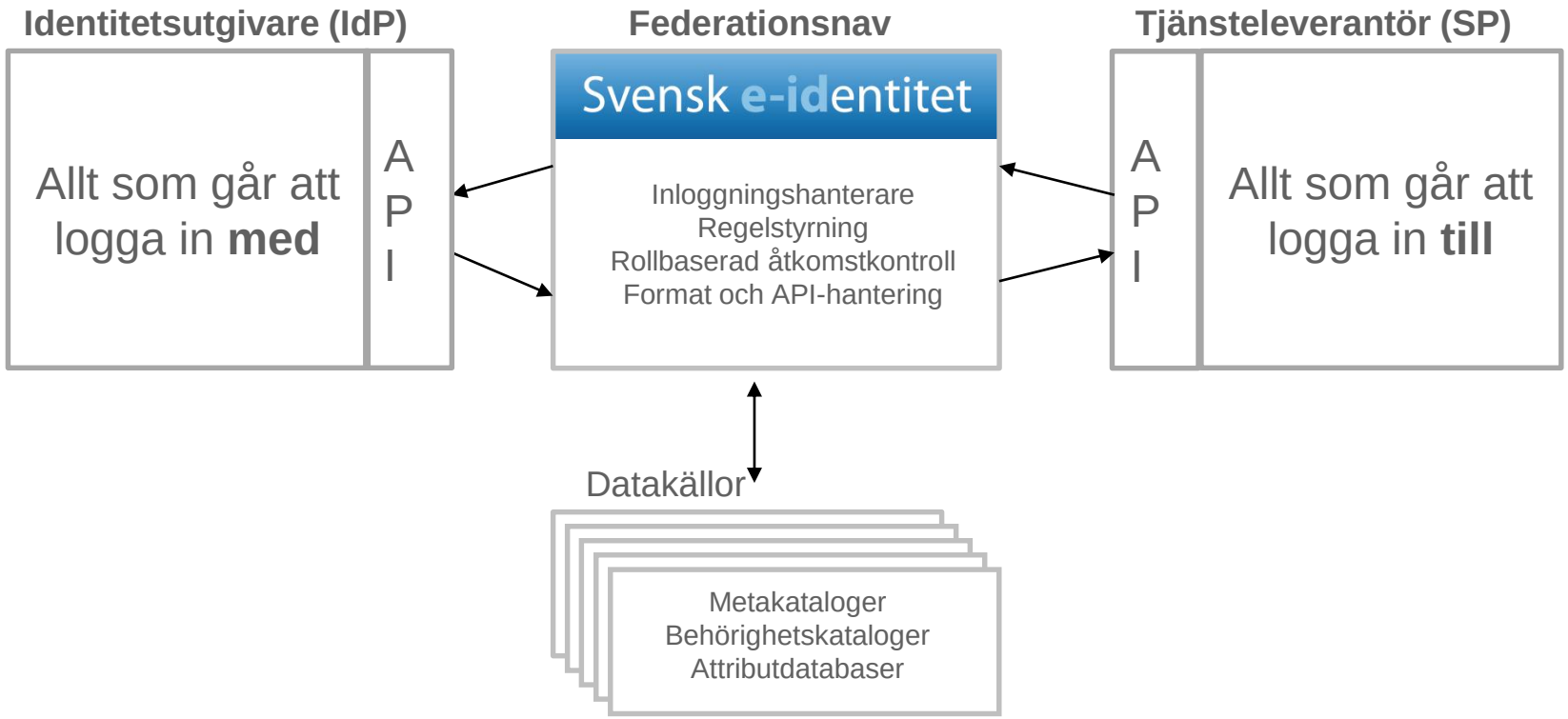
Appar och SAML-federationer i praktiken

Jörgen Hellgren

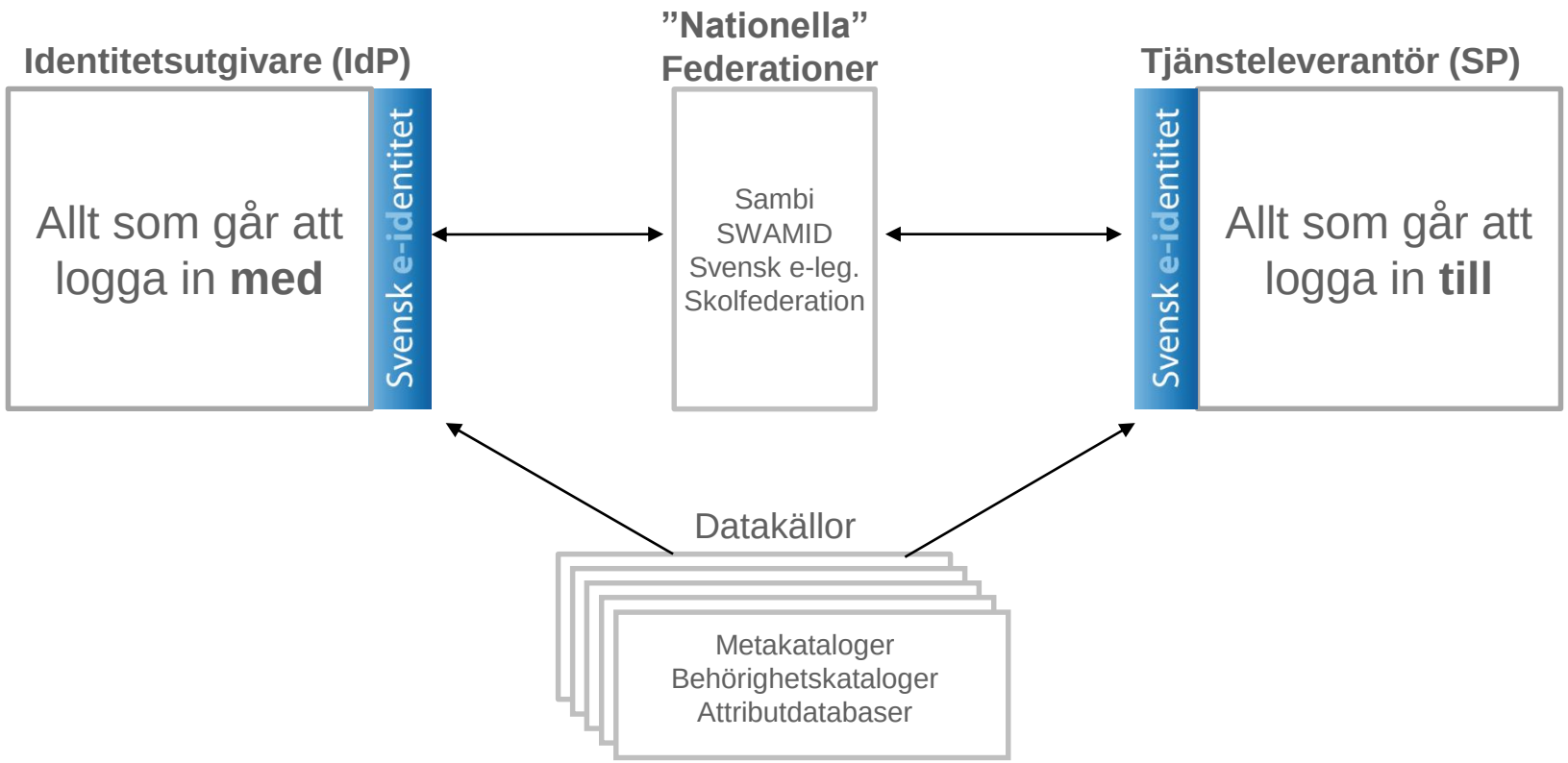
Om Svensk e-identiet AB

- Inloggning och signering som tjänst
- HSA-ombud och utgivare av SITHS-kort

Vår federation



I relation till andra federationer



Demo 1 av 2

SP: Demoapp

Plattform: Native iOS-app

Inloggningsmetod: Testkonto utgivet av .SE

Federation: Skolfederation test

Integrationsmetod: Svensk e-identitets API

YouTube

Demo 2 av 2

SP: DERMICUS (GNOSCO, www.gnosco.se)

Plattform: Native iOS-app

Inloggningsmetod: Mobilt SITHS

Federation: Svensk e-identitet

Integrationsmetod: Svensk e-identitets API

YouTube

Slutsats

Appar och SAML-federationer går att kombinera

Filmer

Svensk e-identitet

Kontakt

Jörgen Hellgren

jorgen.hellgren@e-identitet.se

073-430 18 18

Frågestund







Svenskt federationsforum

Pause

Åter kl 15.45

Varför eduID?

Hans Nordlöf, SUNET

Varför eduID?

Internetdagarna

Svenskt federationsforum 25/11 2014

Hans Nordlöf

hansn@sunet.se

eduID i ett nötskal

- Säker identitetshantering är komplex och dyr
- Genom eduID erbjuds vi säkra och gemensamma id-rutiner – inom hela sektorn
- eduID är en helt öppen IdP, vem som helst kan skaffa ett eduID-konto
- Alla eduID-konton skapas på AL1-nivån
- Proofingmetoder för att elevera till AL2 införs succesivt under året
- eduID är i drift sedan april i år

eduID

- Vad kan man göra med eduID idag?
  - Ger säkert verifierade identiteter på AL2-nivå
  - Aktivera lokala konton på lärosätet
  - Återställa lösenord på lärosätet
  - Målgrupp och fokus på studenter, men det kan ändras
  - Behåller eduID konto ”för evigt”

eduID – fokusområden just nu

- Fler metoder för ID-proofing
- Rejäl ombyggnad av användargränssnittet
- Certifiering för Kantara IAF AL2. Revision andra veckan i december
- Tvåfaktorsautentisiering för helpdesk (RA på lärosätena).
- Attestering/signering med LADOK3?
- Nya tjänster för anställda inom högskolesektorn

SWAMID/eduID

Frågor, tankar, övrigt?

Hans Nordlöf, hansn@sunet.se

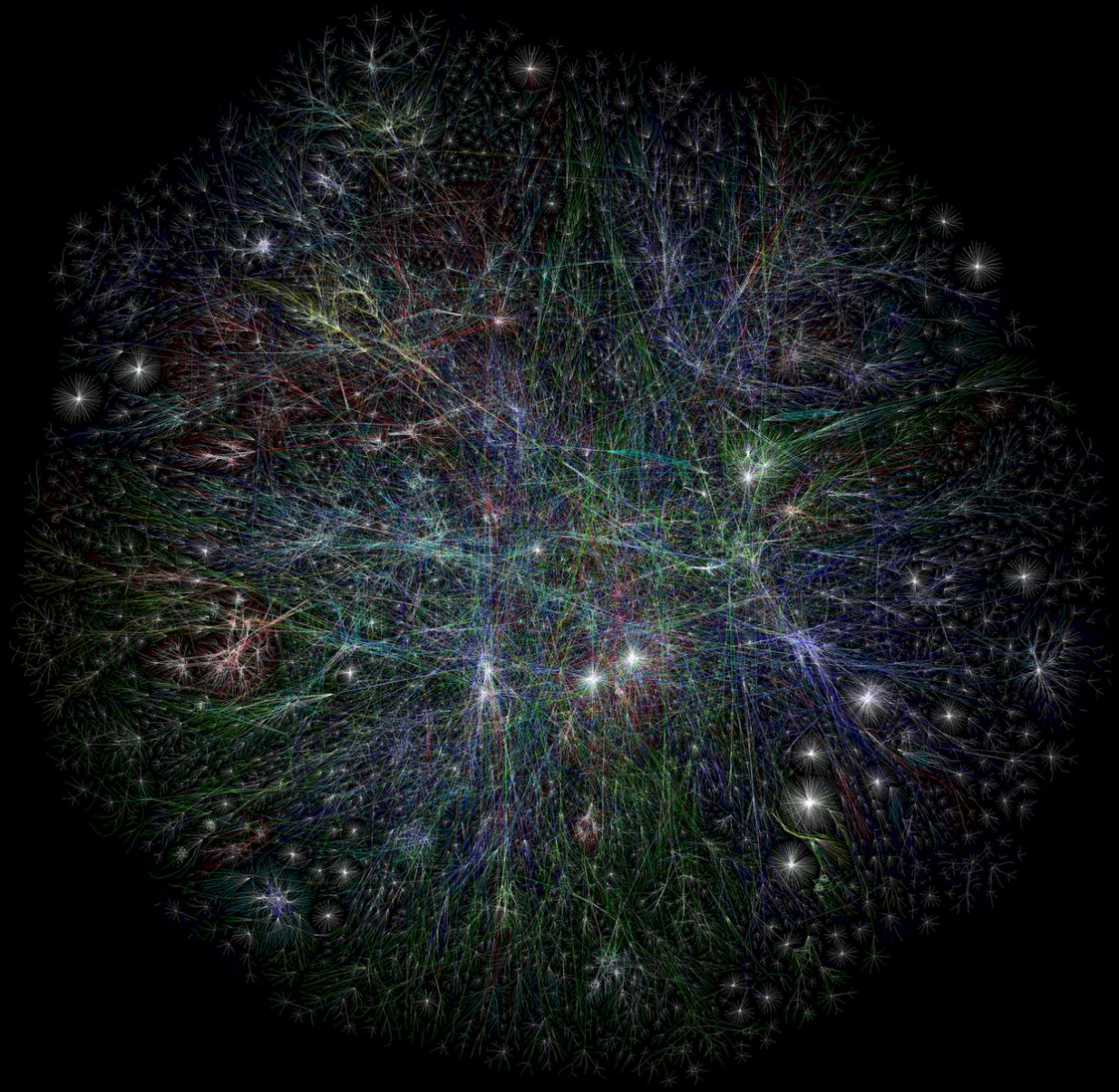
Blixttal fortsättning

Ta tillbaka kontrollen över federerade identiteter och data med SCIM (System for Cross-domain Identity Management)

Erik Wahlström, neXus


nexus
your access to success


SCIM




ORACLE
salesforce
SailPoint
CISCO
nexus
UnboundID
Grouper™
Apache
CLOUD FOUNDRY
ca technologies
IBM
gluu
intel Security
OSIAM
RADIANT LOGIC
One Global Identity to Drive Business in a Distributed W
Ping Identity
Switch Identity Governance
WSO2


Client
Service Provider

```
POST /scim/v2/Users  HTTP/1.1
Host: example.com
Accept: application/scim+json
Content-Type: application/scim+json
Authorization: Bearer h480djs93hd8

{
    "schemas":["urn:ietf:params:scim:schemas:core:2.0:User"],
    "userName":"bjensen",
    ”emails":[
        {
        “value”:babs@jensen.com
        }
    ],
    “active”:true
}
```

```
DELETE /scim/v2/Users/bjensen
Host: example.com
Authorization: Bearer h480djs93hd8
```


12
1
2
3
4
TIMEX

Erik Wahlström

erik.wahlstrom@nexusgroup.com

@erik_wahlstrom

Erfarenheter från arbetet med att uppnå definierad SWAMID AL1-nivå

Pål Axelsson, Uppsala universitet

SWAMID

Erfarenheter från arbetet med att uppnå SWAMID AL1-nivå

Pål Axelsson
Uppsala universitet och
SWAMID Operations

Vad är SWAMID AL1?

- Strukturerad uppsättning av minimikrav som en identitetsutgivare måste uppfylla från och med december 2014 för att kunna användas i den akademiska identitetsfederationen SWAMID.
- Krav på
  - organisation
  - användarhantering
  - teknik
  - säkerhet

SWAMID AL1: https://wiki.swamid.se/display/SWAMID/SWAMID+Identity+Assurance+Level+1+Profile

Erfarenheter runt införande

- Det krävs mycket informations- och stödarbete till identitetsutgivarna för att införa en tillitsnivå
- De flesta kraven är enkla att uppfylla men några aspekter som diskuterats under införandet är
  1. Varför måste vi ha en miniminivå för vår drift?
  2. Varför ska alla användare aktivt godkänna organisationens användarregler, räcker det inte med anställningsavtalet?
  3. Måste inloggnings- och kontohanteringstrafiken mellan servrarna datorhallen vara krypterad, det är ju ett säkert nät?

Erfarenheter runt införande

- SWAMID använde Kantara AL1 som mall för att skriva SWAMID AL1 beroende på att universitet och högskolor verkar i en internationell forskningsmiljö.
  - Ett internationellt ramverk är ibland svårt att sätta i svensk kontext och därför har en del krav blivit svårbegriplig för identitetsutgivarna.
  - En uppdatering av vissa krav kommer behöva göras för att de ska bli enklare att förstå.
- Många identitetsutfärdare har försent insett att de behöver göra åtgärder för att uppfylla kraven.

Sambis nya tillitsramverk

Lennart Beckman, Beckman Security

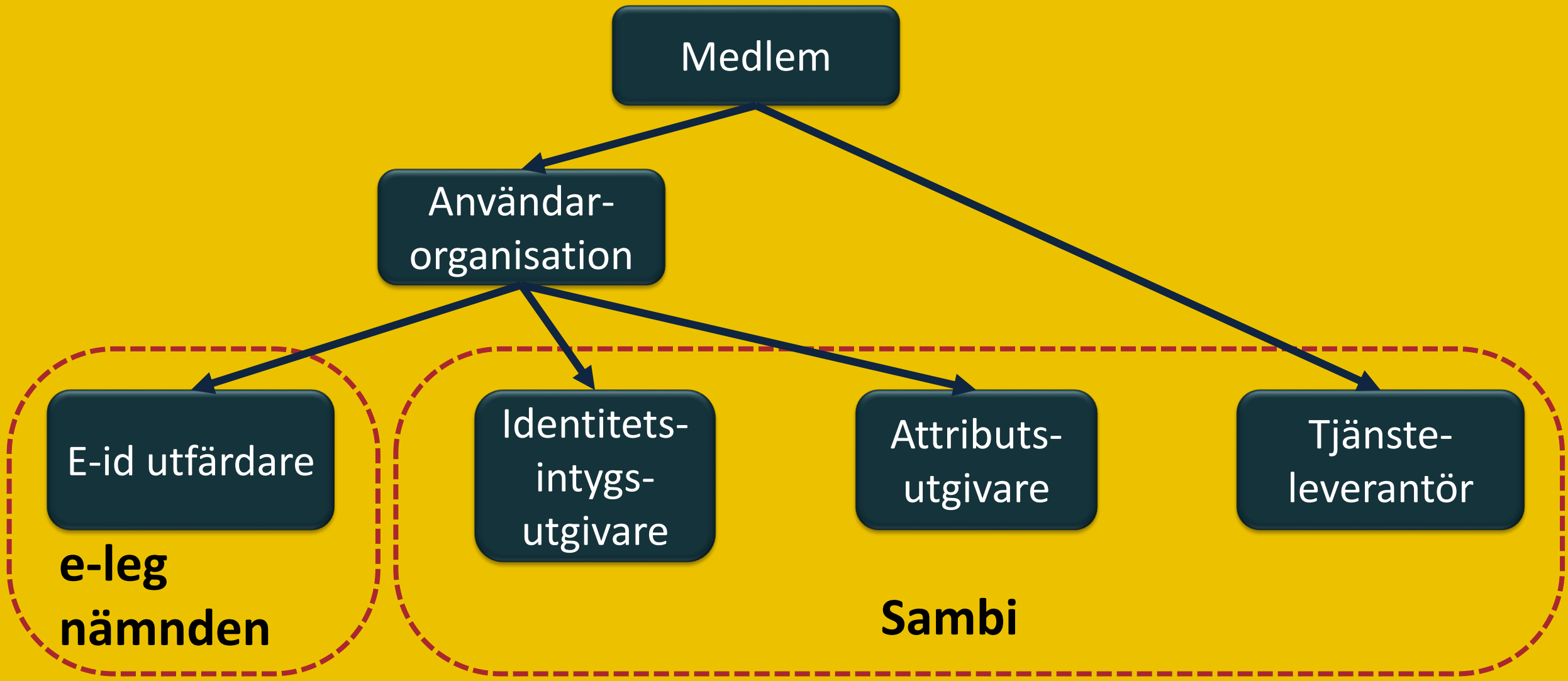
Sambi
Samverkan
för säkrare
e-hälsa

Sambis nya tillitsramverk

Lennart Beckman

Sambi
Samverkan
för säkrare
e-hälsa

Roller, granskning



Sambi
Samverkan för säkrare e-hälsa

Vilken tillit behövs?

- Tjänsteleverantörer ska kunna lita på attribut
- Användarorganisationer ska kunna lita på Tjänsteleverantörens IT-hantering

Sambi
Samverkan
för säkrare
e-hälsa

Tillitsramverket

- Enklare, tydligare
- Baseras i hög grad på Ledningssystem för informationssäkerhet (LIS) enligt ISO/IEC 27000
- Top down i stället för bottom up

Sambi
Samverkan
för säkrare
e-hälsa

Svårt?

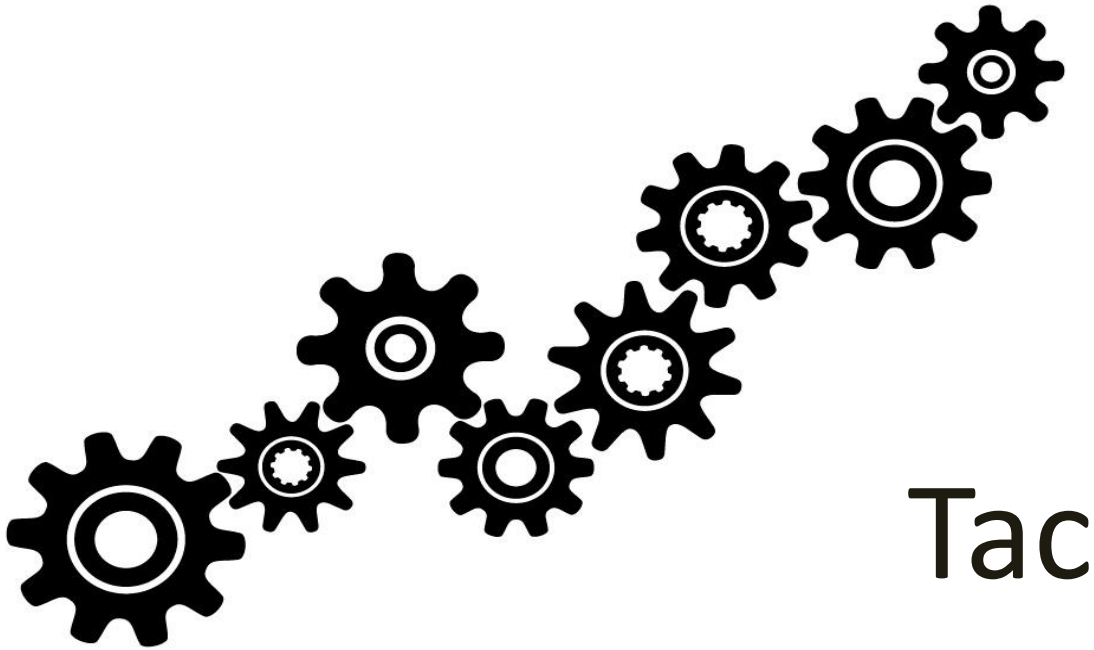
- Enkelt
- Bara för berörda delar av organisationen
- Baseras på riskanalys, anpassas efter verksamheten och hotbilden

Sambi
Samverkan
för säkrare
e-hälsa

Status

- Nytt ramverk snart på plats
  - Krav
  - Definitioner, ordlista
  - Process, organisation
  - Mall för tillitsdeklaration

Sambi
Samverkan
för säkrare
e-hälsa



Tack!

Implementation av eskalerad tillitsnivå från en pilot med Göteborgs stad

Palle Girgensohn, PingPong

SLL, KSL och Sambi ordnar enklare inloggning

Urban Jarl, SLL

Stockholms läns landsting

SLL, KSL och Sambi ordnar enklare inloggning

Urban Jarl, SLL, e-Hälsa och strategisk IT

2014-11-25

Gränsöverskridande processer

Vårt projekt

- SLL
  - IdP
  - användare
  - applikationerna Beställningsportalen och WebCare
- Stockholm stad
  - IdP
  - användare
- Beställningsportalen (SP) utvecklad av Kentor
- WebCare (SP) utvecklad av Tieto
- .SE
  - Anvisningstjänst (DS)
  - Tillit-dokument
  - regelverk

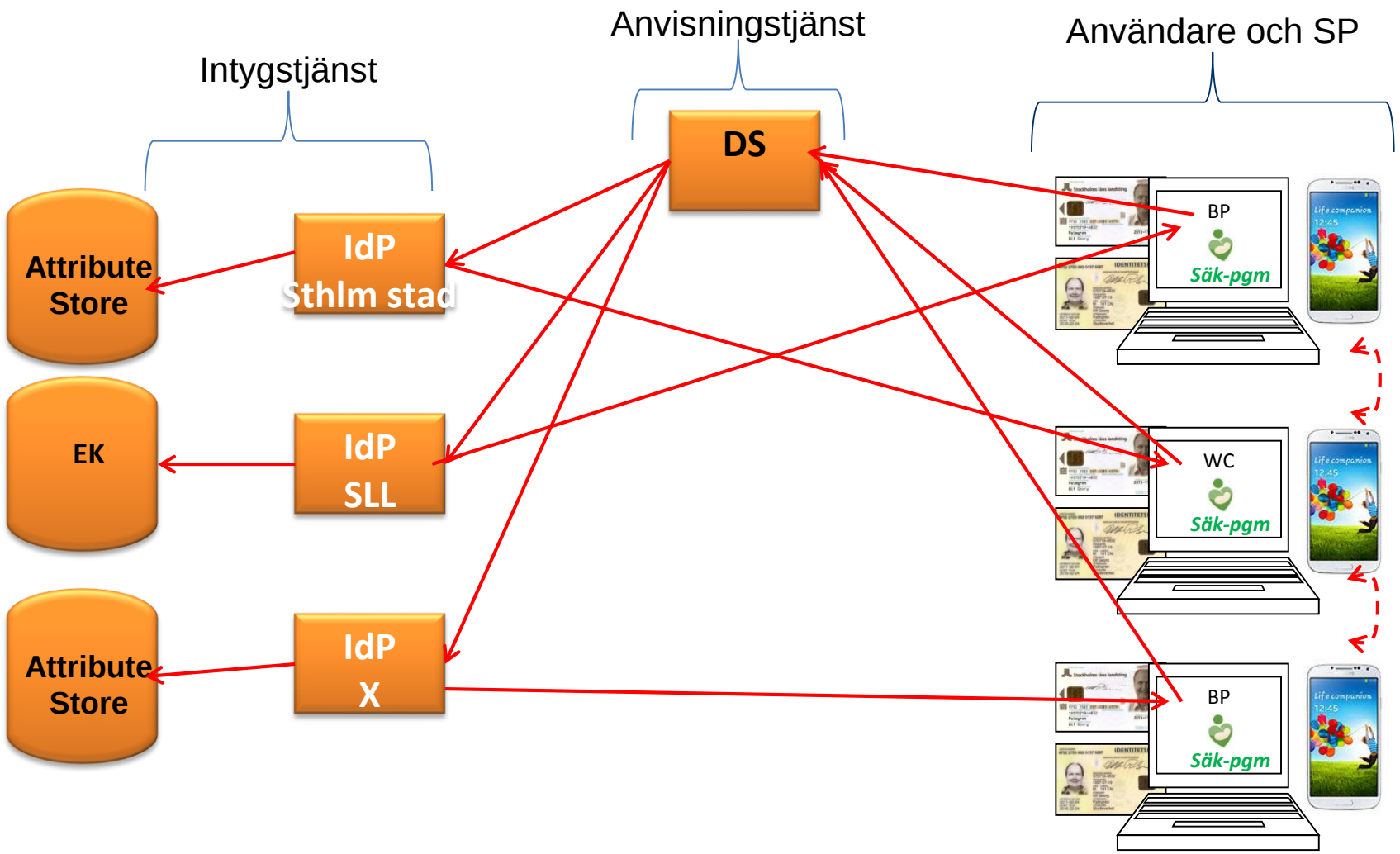
Vårt mål

- Alla användare ska bara
  - finnas registrerade på ett ställe
  - logga in en (1) gång med hjälp av sitt egna organisationskort : Single SignOn

- Ska kunna ”rullas ut” Q1 2015

- Förvaltning inom SLL för egen dokumentation, IdP, Attribute Store och Attribute Authority mm

Vårt projektscenarion



Status idag 1

- SLL
  - pilotanvändare utsedda
- Stockholm stad
  - pilotanvändare utsedda
- Beställningsportalen testad, Tillitsdeklaration gjord
- WebCare ska testas
- .SE
  - håller på att konfigurerar produktionsmiljö för DS
  - håller på att ta fram processer för DS produktionsmiljö

Status idag

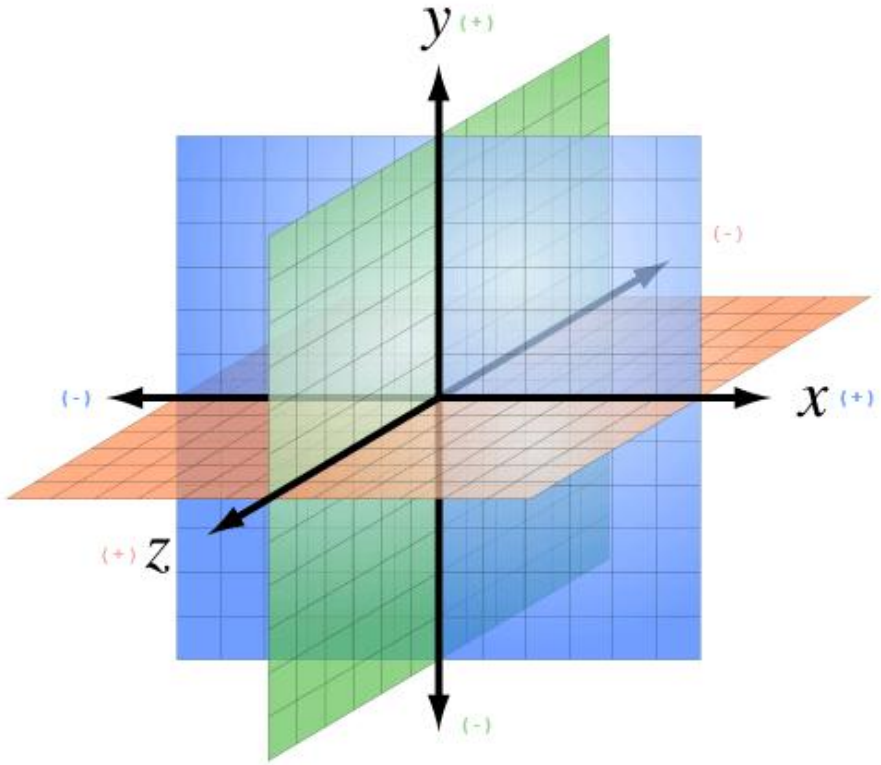
- SLL har
  - tagit fram
    - riktlinjer för SLL-applikationernas attribut
    - checklistor för efterföljande projekt
    - strategidokument
    - utbildningsmaterial (tillsammans med Certezza, E-hälsomyndigheten och .SE), finns på sambi.se
  - förändringsstopp 2014-12-12 – 2015-01-12 klockan 9, i sin produktionsmiljö

Uppkomna saker att lösa

- Sambi Tillits-dokument var inte användningsbart
- Sambis hade ingen produktionsmiljö eller några processer för den
- Sekretess, av till Sambi inlämnade dokument
- Hur ska vi hantera attributen?
- De flesta deltagarna (SLL, Stockholm stad, .SE) har egna ServiceDesk – hur samordnas detta?
- Nordic Edge/McAfee/Intel?
- Utrullning lite i taget

Att tänka på, avseende federation

- *Federation innebär mer än normalt:*
  - 50% processer
  - 50% teknik
    - plus
  - 50% förtroende/tillit



Tack för mig

Frågestund






Summering av dagen

Eva Ekenberg, E-legitimationsnämnden

Jens Lindh, KSL

Leif Johansson, SUNET

Robert Sundin, .SE

Stefan Larsson, eHälsomyndigheten

Valter Nord, SUNET/GÉANT Association

Svenskt federationsforum

Tack för idag och på återseende!